UNIVERSIDAD AUTÓNOMA DE MADRID

ESCUELA POLITÉCNICA SUPERIOR

TRABAJO FIN DE MÁSTER

Autenticación continua de usuario basada en interacción táctil

Máster Universitario en Ingeniería de Telecomunicación

Autor: Moreno de Pablos, Eduardo
Tutor: Morales Moreno, Aythami

Junio, 2018

Autenticación continua de usuario basada en interacción táctil

AUTOR: Eduardo Moreno de Pablos
TUTOR: Aythami Morales Moreno

BiDA-Lab
Dpto. Tecnología Electrónica y de las Comunicaciones
Escuela Politécnica Superior
Universidad Autónoma de Madrid
Junio de 2018

Resumen

Hoy en día, con el auge continuo de la tecnología, cualquier aspecto relacionado con la seguridad adquiere un grado trascendental de importancia. Disponemos de información vital muy sensible en los nuevos dispositivos tecnológicos, ya sean ordenadores, tablets o smartphones. Dicha información debe ser protegida frente a cualquier usuario que no sea legítimo. Para ello, en los últimos años se han utilizado claves, tokens y otros métodos. La parte negativa es que muchos ofrecen un alto porcentaje de vulnerabilidad, además de ser soluciones difícilmente escalables a una vida diaria en la que debemos gestionar un elevado número de servicios y plataformas que requieren protección. Por lo tanto, el reconocimiento biométrico alcanza significativa importancia en este sector, ya que no solo obtiene grandes resultados de cara a proteger la información, sino que, haciendo uso de una parte única correspondiente a nosotros, elimina la necesidad de memorizar una combinación previa o portar un token determinado.

Dentro del reconocimiento biométrico, existen diferentes métodos relacionados con cómo se evalua y/o monitoriza la identidad del usuario. De especial interés para este trabajo es el denominado autenticación continua. Este procedimiento consiste en aplicar una serie de autenticaciones de usuario periódicas de cara a ofrecer mayor robustez, monitorizando de forma constante si el usuario que hace uso del dispositivo analizado es el correcto.

En este trabajo realizado se reflejan detalladamente una serie de estudios y análisis sobre la autenticación de usuarios, focalizándose únicamente en dispositivos con pantalla táctil, en este caso smartphones. Para llevar a cabo este objetivo, se han utilizado medidas obtenidas previamente por diversas fuentes en diferentes bases de datos. Además, se ha hecho uso de algoritmos de clasificación de patrones basados en Máquinas de Vector Soporte y Modelos de Mezclas Gaussianas. Dichos algoritmos explotan la información discriminativa y estadística, para posteriormente combinar sus características mediante la fusión, mejorando de manera notoria los resultados obtenidos.

Finalmente, se ha aplicado el algoritmo denominado *Quickest Change Detection*, el cual incrementa la eficacia del desarrollo en términos de latencia y probabilidad de falsa detección de usuarios. Esto se ha logrado teniendo en cuenta los resultados obtenidos anteriormente al instante en el que el usuario registra nuevos datos en la aplicación.

Palabras clave

Reconocimiento Biométrico, patrones de comportamiento, autenticación continua, interacción táctil, seguridad.

Abstract

Nowadays, with the continuous rise of technology, any aspect related to security acquires a transcendental degree of importance. We have vital information in the new technological devices, whether computers, tablets or smartphones. This information must be protected against any user that is not legitimate. For this, keys, tokens and other methods have been used in recent years. The negative part is that many offer a high percentage of vulnerability, in addition to being hard to scale solutions to a daily life in which we must manage a large number of services and platforms that require protection. Therefore, biometric recognition reaches significant importance in this sector, since it not only obtains great results in order to protect the information, but, making use of a unique part corresponding to us, eliminates the need to memorize a previous combination or carry a certain token.

Within the biometric recognition, there are different methods related to how the identity of the user is evaluated and/or monitored. Of special interest for this work is the so-called continuous authentication. This procedure consists of applying a series of periodic user authentications in order to offer greater robustness, constantly monitoring if the user that makes use of the analyzed device is the correct one.

In this work, a series of studies and analyzes on user authentication are reflected in detail, focusing only on touchscreen devices, in this case smartphones. To carry out this objective, previously obtained measurements have been used by different sources in different databases. In addition, pattern classification algorithms based on Vector Support Machines and Gaussian Mixture Models have been used. These algorithms exploit the discriminative and statistical information, to later combine their characteristics by means of fusion, improving in a noticeable way the obtained results.

Finally, the algorithm called Quickest Change Detection has been applied, which increases the effectiveness of the development in terms of latency and the probability of false detection of users. This has been achieved by taking into account the results previously obtained at the moment in which the user registers new data in the application.

Key words

Biometric Recognition, behavioral biometrics, active authentication, touch interaction, security.

Agradecimientos

En este apartado, quiero agradecer en primer lugar a mi tutor Aythami Morales por brindarme la oportunidad de realizar este Trabajo de Fin de Máster con él y depositar su confianza en mí, además de guiarme constantemente cuando yo lo necesitaba y ofrecerme su apoyo y ayuda. Gracias a él, he aprendido muchos sobre este ámbito, además de mejorar en aspectos como la planificación, organización y redacción, entre muchos otros.

Por otra parte, doy las gracias a todos los profesores que he tenido durante la carrera y el máster. Ellos han contribuido directa o indirectamente en él y en mi formación ofreciéndome respuestas cuando las necesitaba y aclarándome muchísimas dudas.

Por otra parte, y no menos importante, el apoyo de mi familia y seres queridos ha sido vital. Han estado ahí para mantenerme motivado en todo momento y hacer de este proyecto, además de una gran oportunidad de aprendizaje, una gran experiencia vivida.

Eduardo Moreno de Pablos
Junio 2018

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1 Introducción

El presente Trabajo de Fin de Máster propone analizar y desarrollar un sistema de reconocimiento biométrico basado en interacción con pantalla táctil mediante la autenticación continua. Se expone el desarrollo de técnicas de pre-procesado, extracción de características y clasificación que permitan la identificación correcta de un usuario frente al resto. Se trabajará con bases de datos públicas que permita comparar los resultados de este proyecto con propuestas pasadas y futuras. Además del desarrollo algorítmico asociado a la consecución de los objetivos de este TFM, se requerirá un especial esfuerzo de análisis e interpretación de los resultados. Se busca generar nuevo conocimiento que permita avanzar en un campo de especial interés científico y social.

1.1 Motivación

Las nuevas tecnologías han modificado la forma de relacionarse, de compartir información o de realizar tareas, en ámbitos como el entretenimiento, la educación, finanzas, etc. [1]. Este hecho ha sido impulsado en gran medida debido al masivo despliegue de dispositivos móviles como smartphones o tablets. Se puede comprobar como se hace uso de ellos diariamente durante gran parte del tiempo. Además, no solo son utilizados para realizar llamadas o buscar información en internet. También son empleados para albergar o introducir contraseñas, cuentas bancarias, entre muchos otros datos sensibles, en páginas web o aplicaciones [2].

Hoy en día, toda esta cantidad de información puede ser fácilmente perdida o robada. Estudios previos muestran que el 10% de las víctimas de robo telefónico afirman haber perdido información confidencial, un 9% han sufrido robo de identidad y un 12% de las víctimas han experimentado cargos fraudulentos en su cuenta [3]. Este suceso conlleva a hacer uso de sistemas y modelos de seguridad que ofrezcan un alto grado de confianza para que nadie pueda acceder libremente a los dispositivos utilizados.

Para proteger la información y la privacidad del usuario, se implementaron métodos tradicionales como contraseñas, patrones y demás combinaciones de caracteres para poder desbloquear el dispositivo y autenticarse [4]. Garantizar la integridad de estas claves implica la elección de complejas secuencias alfanuméricas, el cambio regular de las mismas, no repetirlas según el servicio o aplicación y memorizarlas en lugar de guardarlas en agendas o similares. Por todo ello, estos códigos tienden a ser de longitud relativamente corta y fáciles de memorizar, conllevando una gran facilidad para romper dicha barrera de seguridad [6].

Con la finalidad de solventar los problemas hallados en los métodos de autenticación comentados previamente, se propusieron modelos de reconocimiento biométricos. Estos modelos utilizan características únicas [6], siendo estos rasgos humanos, entre los cuales se encuentran el iris, huella dactilar, voz, entre muchos otros, con el fin de impedir el acceso a usuarios diferentes. Sin embargo, También son vulnerables a ataques ya que tienen una serie de limitaciones. Por ejemplo, en el desbloqueo mediante huella dactilar, se almacenan residuos en el sensor o pantalla del dispositivo móvil o tablet [2]. Estos restos almacenados ofrecen información vital sobre las características de la huella empleada en el proceso.

Finalmente, se llegó a la conclusión de que los sistemas de verificación de usuario sobre los que se ha hablado con anterioridad, albergan una gran limitación de seguridad. Esta limitación proviene del hecho de autenticarse una única vez al comienzo de cada sesión (*one-shot authentication*) [6]. El usuario no necesita autenticarse de nuevo hasta que el dispositivo sea bloqueado.

Este hecho atrajo el interés de los investigadores con el objetivo de descubrir nuevas formas de autenticarse periódicamente consolidando la seguridad no ofrecida por los otros procedimientos (*active authentication*) [5]. En la figura 1.1 se observa el sistema general típico de autenticación continua [3][1]. En primer lugar, se adquieren los datos del usuario para posteriormente aplicar el algoritmo de autenticación. Si el usuario es correcto, vuelve a adquirir datos sobre él y así sucesivamente. En cambio, si no lo es, el dispositivo se bloquea.

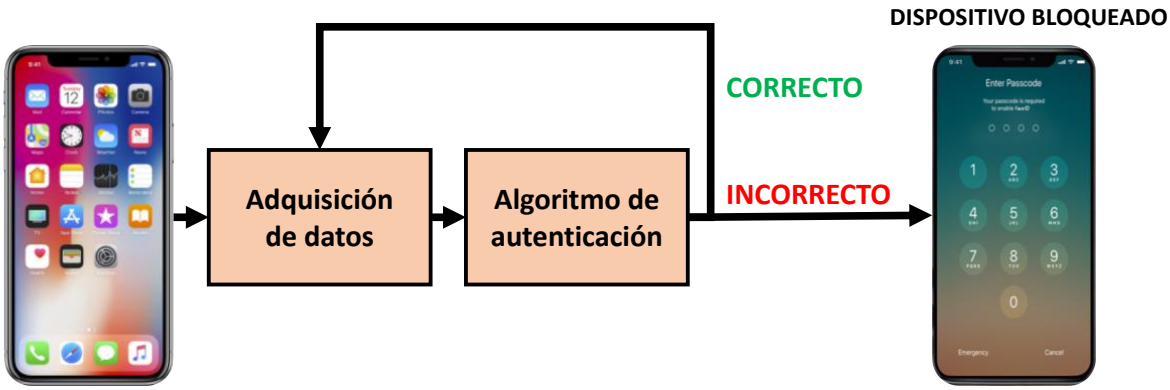

Figura 1.1: Esquema tradicional de autenticación continua.

Centrándose en dichos estudios, la autenticación continua de usuario basada en interacción táctil es uno de los campos que ha ocupado mayor protagonismo. Como se ha comentado anteriormente, el objetivo que persigue esta área es autenticar de forma pasiva al usuario mediante los gestos realizados sobre el dispositivo móvil mientras interactúa con él, sin necesidad de utilizar un sensor no emplazado en el Smartphone [6].

Este procedimiento ofrece un grado de discriminación entre usuarios medio-alto, aunque no comparable a rasgos biométricos tradicionales como la huella dactilar y el iris. En la figura 1.2 se muestran los trazos de 8 usuarios diferentes, obtenidos mientras estos leían diferentes textos en un dispositivo móvil. En esta ilustración, las diferencias entre los gestos realizados por los usuarios son notables.

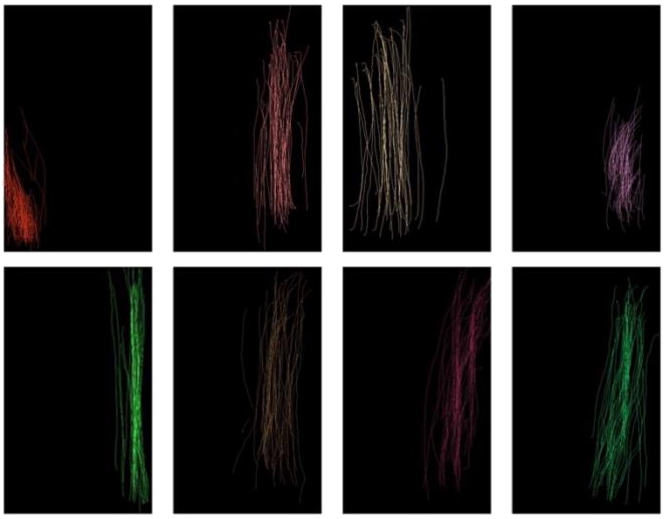

Figura 1.2: Comparativa trazos entre diferentes usuarios. Fuente: [7]

No obstante, este sistema también presenta una alta variabilidad intra-clase [2], en función del momento, la tarea o estado emocional en el que se encuentre el usuario. En la figura 1.3 se visualizan los trazos de dos usuarios en diferentes días, dónde los datos en verde y en negro se corresponden a días diferentes, apreciándose notables desigualdades. A pesar de ello, los gestos realizados por un usuario tienden a ser estables en el mismo día.

En este contexto cabe destacar el conjunto de desafíos principales que alberga el tema tratado [2]. En primer lugar, no se puede alcanzar grandes cuotas de precisión debido a las limitaciones presentes en los dispositivos móviles. Este hecho se está solventando reduciendo la cantidad de falsos positivos y negativos mediante nuevas propuestas de características y clasificadores. En segundo lugar, la latencia es un factor fundamental en la autenticación continua. El tiempo de detección no debe ser ni demasiado lento, donde el intruso tendría suficiente tiempo para extraer información, ni demasiado rápido, ya que el sistema detectaría resultados de periodos cortos e insuficientes. Por último y no menos importante, la eficiencia del modelo implementado, es decir, cuantos recursos (memoria, batería, etc.) consumirá este.

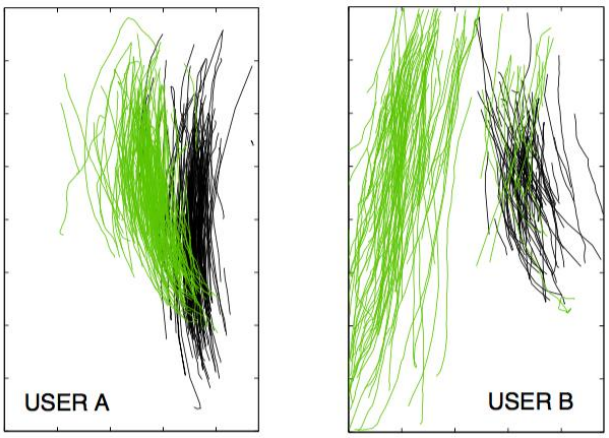

Figura 1.3: Comparación de trazas obtenidas por dos usuarios en diferentes días. Fuente: [2]

1.2 Objetivos y metodología

El presente TFM pretende avanzar en el estudio de la autenticación continua a partir de la interacción táctil. Se analizarán nuevas metodologías que permitan incrementar la eficacia de autenticación de usuarios de forma continua, basándose en los estudios previos ya comentados, así como un Trabajo de Fin de Grado previo [6]. Uno de los retos consiste en la integración temporal de la información obtenida a partir de la interacción táctil de cara a aumentar la robustez del algoritmo de autenticación. Dentro del objetivo general mencionado con anterioridad, se han establecido una serie de objetivos parciales a medio y largo plazo:

- Documentarse correctamente y aprender sobre el área de investigación en cuestión. En primer lugar, con conceptos básicos, mediante la lectura del libro recomendado [8]. Posteriormente, con el estudio de los diferentes artículos de investigación ofrecidos por el tutor [5][9][10][7], de cara a profundizar mayormente en el contexto del trabajo realizado.

- Familiarizarse con el código básico suministrado, correspondiente mayoritariamente al realizado en el trabajo previo [6], así como mi tutor, para posteriormente poder mejorarlo y modificarlo con el objetivo de obtener la finalidad propuesta. En dicho trabajo se desarrollaron técnicas de modelado de los gestos táctiles de los usuarios para su autenticación. El objetivo de este TFM es avanzar en esta línea, analizando y estudiando

esquemas de autenticación continua basados en los modelos propuestos en [6].

- Desarrollar y analizar metodologías de autenticación continua basada en rasgos biométricos obtenidos a partir de la interacción táctil.

    - Se han utilizado 3 bases de datos públicas a partir de las cuales poder garantizar la reproducibilidad de todos los experimentos. Dichas bases de datos son representativas de diferentes escenarios y metodologías de adquisición de interacción táctil..
    - Se ha implementado el algoritmo de autenticación continua propuesto en [3] conocido como Minimax QCD-Based Intrusion Detection.

- Analizar todos los resultados de forma global para obtener conclusiones de cara a optimizar lo ya estudiado y extraer conocimiento.

Para llevar a cabo y cumplir los objetivos establecidos, se define a continuación la metodología y plan de trabajo empleados. En esta lista se enumeran las tareas principales realizadas, además de las subtareas correspondientes a cada una de ellas. En la figura 1.4 se muestran las horas empleadas en las tareas principales, sumando en total de 300 horas correspondientes a 12 ECTS.

1. **Documentación previa y código (lectura y estudio).**
    1.1. Bibliografía recomendada [5][9][10][7][3][8][11].
    1.2. Estudiar las diferentes bases de datos a utilizar.
    1.3. Comprender código suministrado.
2. **Desarrollo de algoritmos de autenticación continua.**
    2.1. Algoritmos de comparación.
    2.2. Algoritmos para la evaluación de rendimiento de sistemas de autenticación continua.
3. **Obtención de resultados.**
    3.1. Diseño del protocolo experimental.
    3.2. Obtención de resultados, tanto numéricos como gráficos.
4. **Análisis y conclusiones sobre los resultados obtenidos.**
5. **Realización memoria del trabajo.**
6. **Desarrollo documento presentación y defensa pública del trabajo.**

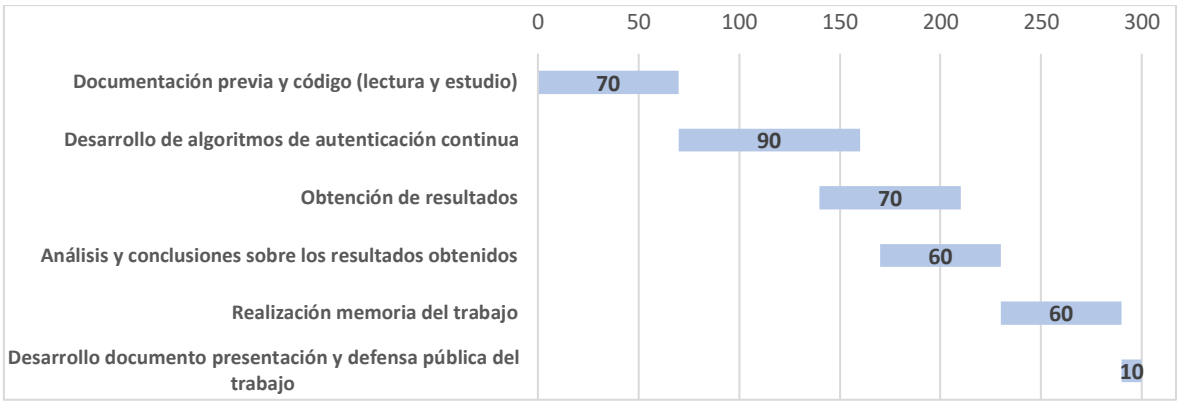

Figura 1.4: Cronograma del Trabajo de Fin de Máster

1.3 Organización de la memoria

La memoria consta de los siguientes capítulos:

- **Capítulo 1. Introducción**. En esta sección, aparte de introducir la materia en cuestión, se incluye la motivación, objetivos y metodología de este trabajo.
- **Capítulo 2**. **Estado del arte**. Este apartado se integra por el conjunto de documentos científicos y trabajos estudiados y analizados de cara a sentar las bases y poder realizar este Trabajo de Fin de Máster.
- **Capítulo 3. Diseño**. En dicho capítulo se exponen el conjunto de bases de datos utilizadas, así como los algoritmos de reconocimiento biométrico, de autenticación continua y el protocolo de evaluación de los experimentos realizados.
- **Capítulo 4. Resultados experimentales**. Como bien indica el título de esta sección, se incluyen el grupo de resultados, en forma de gráfica, tabla o mapa de calor, de los experimentos llevados a cabo.
- **Capítulo 5. Conclusiones y trabajo futuro**. Finalmente, se procede a resumir el trabajo realizado y se exponen nuevas ideas para incrementar y mejorar el trabajo desempeñado.

2 Estado del arte

En esta sección se mencionan las ideas y conceptos de una serie de artículos y trabajos estudiados en relación con la autenticación continua y demás aspectos introducidos previamente.

En [5], el objetivo principal de los autores consiste en analizar toda la información proveniente de gestos simples realizados con el dedo como movimientos horizontales o verticales sobre una pantalla táctil. Se ha deducido que todos estos datos contienen gran información del usuario en sí, como puede ser la identidad, el género o el nivel de experiencia de este. Además, se afirma que a mayor cantidad de información se dispone del usuario, se obtiene mayor precisión en la identificación.

Las mediciones se hicieron mediante la recopilación de datos de 71 usuarios usando 8 dispositivos móviles diferentes. Los datos obtenidos se dividieron en trazos o *strokes*, para así poder realizar una clasificación basada en trazos individuales o múltiples, siendo estos últimos mucho más precisos, alcanzando un 100% de acierto con un conjunto de 20 trazos, en comparación con los individuales, donde se obtiene de media un 65%.

Por otra parte, se obtienen altas cuotas de clasificación correcta entre hombres y mujeres, siendo estas en torno al 88%. La principal diferencia que se advierte entre los trazos de hombres y mujeres es que los primeros tienden a realizar movimientos más cortos y menos rectos. Igualmente, los usuarios menos experimentados son propensas a desarrollar recorridos más largos con mayor velocidad.

Para realizar las comparaciones y obtener el conjunto de resultados mencionado, definen un modelo de extracción de características con una serie de elementos. Entre estos se encuentran las coordenadas x e y de comienzo y fin, la longitud del segmento, desviación, entre otros. Varias de estas características se ilustran en la figura 2.1.

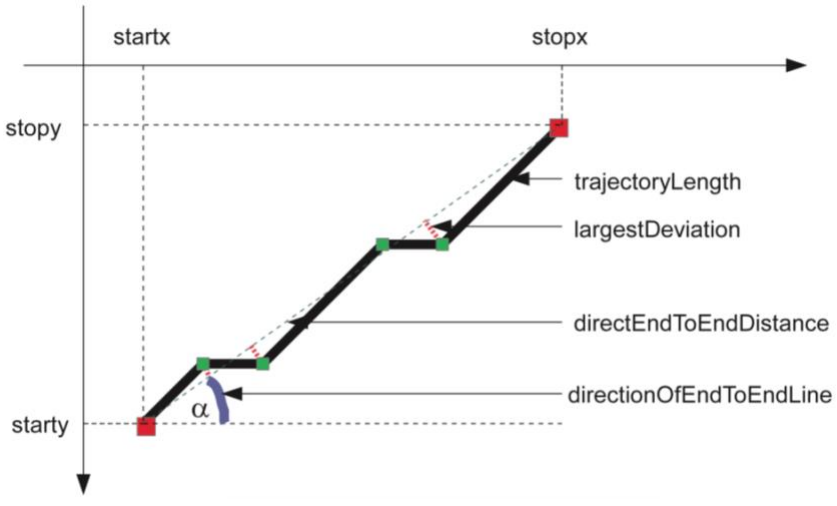

Figura 2.1: Características extraídas de los trazos almacenados. Fuente: [5]

En la mayoría de experimentos que han sido realizado sobre este ámbito en concreto, las técnicas y métricas empleadas varían notablemente entre sí. Además, los resultados no son fácilmente accesibles de forma pública.

Por lo tanto, la investigación propuesta en [9] se focaliza principalmente en dos secciones. La primera de ellas consiste en obtener una comparación de rendimiento de 10 algoritmos de clasificación basados en la autenticación táctil bajo un protocolo experimental común. Esa comparación se llevó a cabo mediante la equiparación de los *Equal Error Rate* (EER) resultantes de cada algoritmo. De los 10 examinados, 5 de ellos no habían sido estudiados previamente. Este proceso se llevó a cabo gracias al uso de bases de datos públicas. La segunda sección consiste en descartar los usuarios cuyos EER sean superiores a una serie de umbrales establecidos. Este fenómeno es conocido como "*failure tu enroll*". La finalidad de este segundo apartado consiste en averiguar cuanta mejora se alcanzará prescindiendo de usuarios con resultados inferiores al valor requerido, para así poder estimar que porcentaje de la población podría utilizar el modelo propuesto.

En la figura 2.2 se contemplan, para 3 algoritmos de los 10 utilizados en [9], como varía el EER en función del umbral utilizado en ese instante. Al aplicar el umbral y descartar los usuarios con malas puntuaciones, se vuelven a recalcular los EER. Se aprecia como mejoran contundentemente los resultados, siendo dicha mejora más pronunciada en los trazos horizontales.

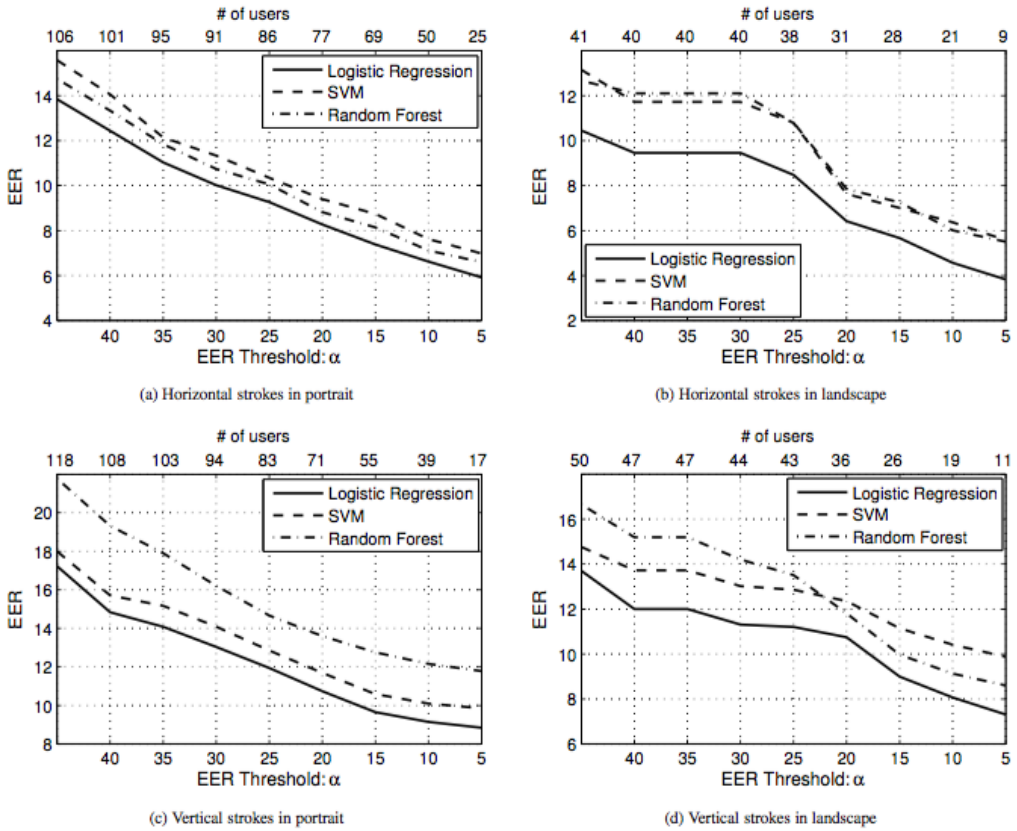

Figura 2.2: Variación de los EER obtenidos de 3 algoritmos de los 10 utilizados en función del umbral aplicado. Fuente: [9]

En [10], se concentran en continuar la investigación de técnicas de verificación de usuario para smartphones, focalizándose no solo en un modo de autenticación continua por medio de gestos táctiles, si no que ofrecen una serie de alternativas, como por ejemplo la cámara delantera o el servicio de ubicación.

En este caso concreto, el rasgo biométrico más utilizado en la base de datos ha sido el rostro. Principalmente, la cara ha presentado un conjunto de dificultades debidas a diferentes poses, oclusiones o desigualdades de iluminación.

Dentro de la autenticación táctil, para estudiar los trazos realizados por los usuarios, se han introducido tres tipos de eventos, los cuales son la pulsación del dedo sobre la pantalla, el mantenimiento de este y el posterior alzamiento. Al no estar la base de datos dividida en diferentes sesiones como ocurría con otros documentos científicos estudiados [9][7], en primer lugar, se ordenan los datos almacenados cronológicamente para después dividirlos en muestras de entrenamiento y test en una proporción 70%-30%, respectivamente.

Finalmente, en vez de tener en cuenta un único deslizamiento de para los resultados, se define una variable denominara W_{swipes}, siendo esta el número de trazos promediados entre sí para ofrecer mayor robustez en la solución. En la figura 2.3 se puede comprobar dicha robustez, ofreciendo una notable mejorar en los EER obtenidos para los diferentes algoritmos utilizados.

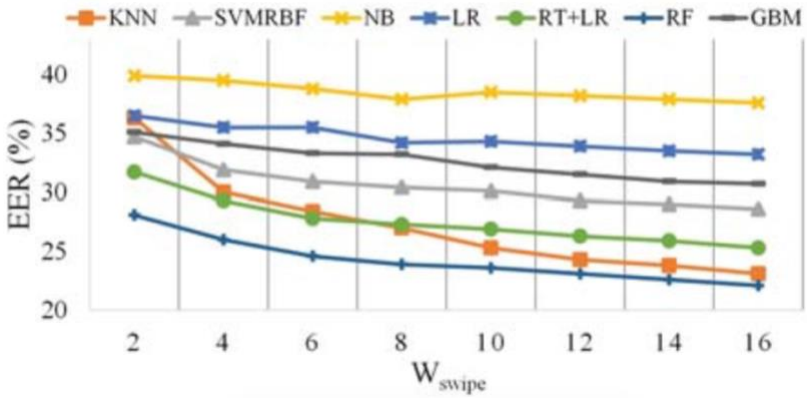

Figura 2.3: EER vs W_{swipes}. Fuente [10]

En [7] prosiguen con el estudio sobre la posibilidad de autenticar usuarios mediante la forma que tienen de interactuar con la pantalla de un Smartphone. Para ello, proponen un conjunto de 30 características extraídas de los comportamientos táctiles de los usuarios, demostrando que diferentes personas ocupan subespacios dispares dentro del conjunto de características mencionado.

Por otra parte, presentan métodos de clasificación que aprenden del comportamiento del usuario en una fase de autenticación, además de estudiar la consistencia de los resultados a lo largo del tiempo, recolectando datos de los usuarios analizados en diferentes sesiones. Los resultados obtenidos en este estudio reflejan un rendimiento mayor en autenticaciones intra-session, obteniendo un EER igual a 0%, inferior en autenticaciones inter-sesión, donde los valores de EER se sitúan entre 2% y 3%, y peor en autenticaciones llevadas a cabo después de una semana del registro de los usuarios, en el cual se alcanzan EER por debajo del 4%.

Dentro de la autenticación continua, proponen dos fases:

- **Fase de inscripción o Enrollment Phase:** en esta etapa, el sistema debe ser entrenado por el usuario mediante un método de autenticación convencional. Mientras el usuario se autentica, el sistema extrae una serie de características. El proceso termina cuando almacena un conjunto de rasgos necesarios con los que se pueda discriminar a la persona frente al resto.

- **Fase de autenticación continua:** una vez que el clasificador esté entrenado, comienza el procedimiento de verificación del usuario. Si este no es el usuario legítimo, el sistema retorna a la fase 1. Dependiendo de la precisión del clasificador, se necesitarán más o menos trazos para autenticar al usuario.

En la figura 2.4 se muestran una serie de características de los trazos proyectadas en un subespacio de dos dimensiones. Los datos han sido recolectados de usuarios mientras leían diferentes artículos de Wikipedia. Cada usuario tiene un número de color diferente. En la gráfica de la izquierda se presentan la presión ejercida por el dedo en la mitad del trazo frente a la duración de este. En cambio, en la gráfica de la derecha se exponen las coordenadas X e Y del primer contacto de dicho dedo con la pantalla. A pesar de ser el subespacio únicamente bidimensional, se empiezan a apreciar evidentes separaciones entre clases.

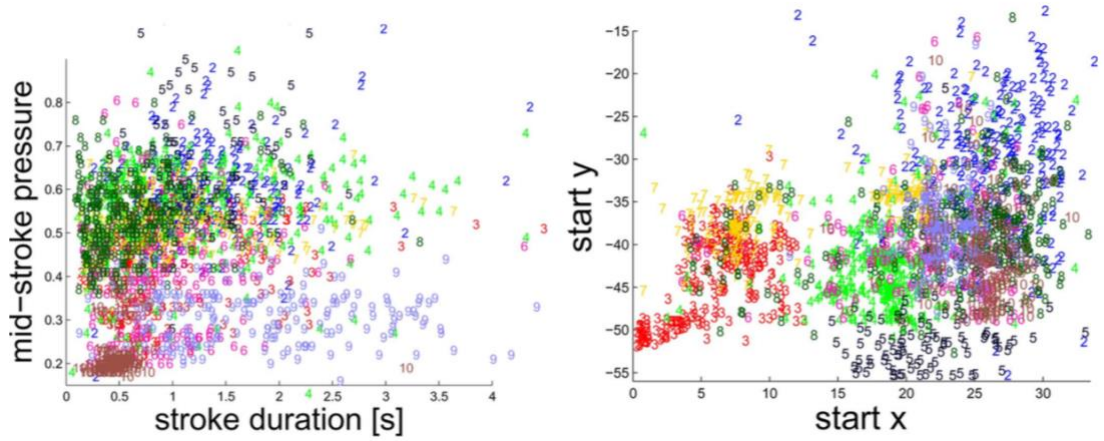

Figura 2.4: Características de trazos de usuarios en subespacio 2-D. Fuente [7]

Especialmente, [3] y [1] han sido trabajos muy importantes para este TFM. Las razones principales se esclarecen a continuación.

En primer lugar, se definen nuevos métodos para aumentar la velocidad de detección de intrusos con una probabilidad de falta detección reducida. Este proceso se lleva a cabo mediante la utilización de un algoritmo denominado Quickest Change Detection (QCD) y una serie de variantes sobre este. Para cumplir con los objetivos prestablecidos, el modelo presentado tiene en cuenta los deslizamientos realizados en el pasado, guardando sus valores correspondientes y sumando a estos los futuros resultados. Cuando el valor final obtenido por el algoritmo supere un umbral establecido de forma previa, el usuario será considerado como impostor. Se ha demostrado como el método propuesto obtiene un mayor rendimiento en términos de latencia y probabilidad de falsa detección, comparándolo con otros métodos tradicionales de autenticación continua.

En la figura 2.5 se muestra un ejemplo utilizado en [1] en donde se aplica el algoritmo QCD al reconocimiento facial en smartphones. Principalmente, se visualiza de forma clara como en momentos donde el usuario inicial mantiene una pose de cara parecida (frames A, B, C y transición de I a J), el valor obtenido por el algoritmo es relativamente pequeño. Sin embargo, cuando el usuario cambia la pose de su rostro, el resultado obtenido es mayor sin sobrepasar el umbral (frames D, E, F, G y H). Finalmente, cuando se introduce en el escenario una persona diferente (frames I, J y K), el algoritmo muestra un resultado mayor que el umbral prestablecido.

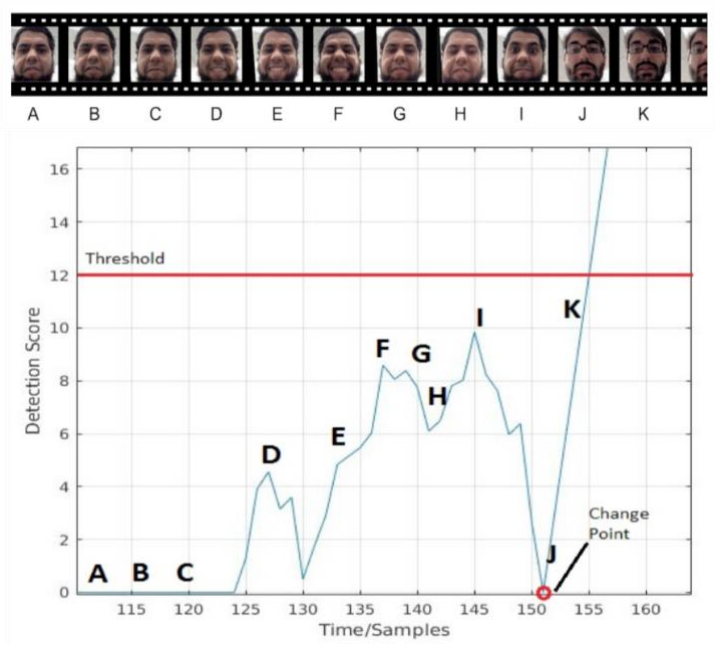

Figura 2.5: Muestras de caras de usuarios frente a resultados obtenidos por algoritmo QCD. Fuente: [1]

Concretamente, en [1] se definen dos variables para evaluar el rendimiento de un sistema de autenticación continua:

- **Average Detection Delay (ADD):** es el tiempo promedio (medido en número de muestras necesarias) que tarda en detectarse un intruso. Cuanto menor sea ese retardo, la eficacia obtenida será mayor.
- **Probability of False Detections (PFD):** Como sus siglas indican, es la probabilidad de falsa detección, es decir, la probabilidad de que se detecte a un usuario correcto como impostor. Es necesario que este parámetro adquiera un valor relativamente menor para no importunar la usabilidad de la persona perteneciente al dispositivo examinado.

Las dos variables comentadas previamente, así como el algoritmo QCD y los métodos propuestos en el documento analizado, se detallarán de manera más exhaustiva en la siguiente sección.

En gran parte del Trabajo de Fin de Máster realizado se ha utilizado información y se ha tomado como referencia el Trabajo de Fin de Grado [6] y su correspondiente artículo científico mencionado en esta sección [4].

Dentro del campo de la autenticación del usuario mediante gestos táctiles, se explora un enfoque estadístico basado en Modelos de Mezclas Gaussianas (GMM) con la adaptación del Modelo Universal de Background (UBM). El objetivo consiste en modelar el comportamiento de los usuarios y como se distribuyen sus datos. Además, se afirma que los trazos en horizontal son más discriminativos con respecto a los trazos realizados en vertical.

En el sistema empleado, el procedimiento consta en primer lugar de un preprocesado de la información proveniente del smartphone. Se considera por separado la posición del dispositivo, es

decir, si se encuentra en horizontal o en vertical. Asimismo, Se clasifican los movimientos en cuatro grupos, según su dirección. Posteriormente, se extraen el conjunto de características definidas previamente. Finalmente, se combinan las características obtenidas con un modelo universal (UBM). Para ello, se define un factor de relevancia, cuyo valor influenciará en la composición comentada anteriormente. Si este valor es alto, se dará mayor importancia al modelo UBM y viceversa.

En el momento en que sea necesario autenticar a un usuario, se extraerán las características de sus trazos realizados y se comprobará el grado de similitud con el modelo previamente establecido. Si no hay suficientes semejanzas, el dispositivo se bloqueará impidiendo el acceso a dicha persona.

Consecutivamente a este artículo, se realizó uno nuevo [2] ampliando las ideas originales con nuevas metodologías. A parte de utilizar modelos GMM, se emplearon por separado Máquinas de vectores de soporte (SVM), con el objetivo de realizar una fusión de ambos esquemas. Además, se estudiaron escenarios intra-session e inter-session, donde los resultados a comparar provienen del mismo día o de días diferentes, respectivamente.

Finalmente, en la tabla 2.1 se recogen el conjunto de trabajos descritos en esta sección junto a otros sobre los que no se ha entrado en profundidad. En ella se encuentran el número de usuarios de cada base de datos, el número medio de trazos por usuario, los clasificadores empleados, los resultados obtenidos y otra serie de características.

					Performance (%)	
Study	**# users**	**# strokes/user**	**# features**	**Classifiers**	**Intra-session**	**Inter-session**
Frank et al. [7]	41	488	27	SVM, kNN	EER: 2.0-3.0	EER: 0.0-4.0
Serwadda et al.[9]	190	400	28	Ten different clasiffiers (best logistic regression, SVM and random forest)	-	EER: 13.8-36.0
Xu et al. [12]	32	200 (29 users), 1200 (3 users)	37	SVM	EER: 10.0	Acc: 70.0-100.0
Zhang et al. [13]	50	-	27	SVM, sparsity-based classifiers	EER: 4.1-5.9	EER: 4.9-14.4
Kumar et al. [14]	28	175	5	kNN, random forest	Acc: 88.0-92.0	-
Mahbub et al. [10]	48	3482	24	kNN, SVM, GBM random forest	EER: 22.1-38.0	-
Shen et al. [15]	71	2002	22-27	SVM, random forest, kNN, neural networks	FAR: 1.9-7.4 FRR: 2.7-8.6	FAR: 4.7-10.9 FRR: 5.7-13.5

Tabla 2.1: Recopilación de diferentes trabajos realizados. Fuente: [2]

3 Diseño

3.1 Bases de datos empleadas

A continuación, se describen y se exponen las características de las bases de datos utilizadas para los experimentos incluidos en este Trabajo de Fin de Máster.

3.1.1 A. Serwadda *et al.* [9]

Para recolectar el conjunto de datos requeridos, los autores desarrollaron dos aplicaciones Android en las que el usuario debía responder a una serie de cuestiones. Para poder contestar a dichas cuestiones, los usuarios debían realizar una serie de gestos. Ejemplos de gestos realizados serían efectuar trazos sobre la pantalla táctil del dispositivo, tanto en horizontal como en vertical.

A la vez, la aplicación obtiene una serie de características sobre los datos almacenados, agrupándose en dos bloques en función de si los trazos realizados son horizontales y verticales.

En esta base de datos se incluyen patrones de 190 estudiantes o miembros de Louisiana Tech University, siendo el modelo usado un Google Nexus S. Los datos fueron capturados en dos sesiones con un día de diferencia entre ellos. Solo se obtuvieron datos producidos por interacción con un único dedo.

3.1.2 M. Frank *et al.* [7]

En la base de datos propuesta en [7], se adquirió información de 41 asistentes. Se utilizaron un total de 4 smartphones cuyos sistemas operativos son Android. Se escogieron únicamente cuatro dispositivos para eliminar cualquier influencia producida por la utilización de diferentes tecnologías. Los datos fueron capturados en dos sesiones, con una semana de diferencia entre ellas. Las características se adquirieron gracias a una API estándar de Android.

Los experimentos para adquirir la información consistieron en la utilización de una serie de aplicaciones donde los usuarios debían realizar un conjunto de tareas. Este conjunto de cometidos consistía en leer tres documentos para posteriormente responder una serie de preguntas acerca de estos. Posteriormente a estos ensayos, debían comparar diferentes imágenes muy similares entre sí. Todos estos procedimientos se instauraron de manera que las personas implicadas tuviesen que realizar una serie de trazos en la pantalla previamente establecidos. Asimismo, no hubo restricción con respecto a la colocación de los smartphones. Estos se pudieron utilizar tanto en vertical como horizontalmente.

3.1.3 UMDAA-02 [10]

En la base de datos propuesta en [10] se obtuvieron datos y características sobre 48 usuarios. El modelo de móvil utilizado fue un Nexus 5.

El proceso de adquisición de información se realizó en un periodo de 2 meses. Los datos se almacenaron en varias sesiones. En este caso, una sesión comienza desde que el usuario desbloquea el móvil hasta que lo vuelve a bloquear. A parte de obtener información sobre los gestos táctiles propiciados por el conjunto de personas implicadas en el experimento, se adquieren

datos provenientes de la cámara delantera, acelerómetro, sensor de luz, GPS, Bluetooth, entre otros.

A diferencia de las demás bases de datos [5][9][7], no se focalizan en la ejecución de una serie de tareas de cara a abastecer de información al experimento. En este caso, los usuarios emplearán los smartphones suministrados como dispositivos móviles principales, utilizándose estos en su día a día.

A continuación, se listan el conjunto de rasgos que se obtuvieron en todas las bases de datos.

- Coordenadas X e Y de todos los puntos definidos en el trazo realizado.
- Presión ejercida del dedo sobre la pantalla.
- Área cubierta por el dedo.
- Orientación del dedo respecto a la pantalla.
- Orientación de la pantalla, es decir, si el móvil se encuentra dispuesto en horizontal o en vertical.
- Tiempo total en el que el dedo ha estado interactuando sobre la pantalla.

En la siguiente tabla se resumen las principales características de las bases de datos mencionadas anteriormente.

Bases de datos	Número de usuarios	Sesiones	Tiempo entre sesiones	Supervisado
Serwadda	190	2	1 día	Si
Frank	41	2 (una semana entre medias)	1 semana	Si
Antal	71	Múltiples sesiones durante 4 semanas	No existe un tiempo establecido entre sesiones	Si
UMDAA-02	48	Múltiples sesiones durante 2 meses	No existe un tiempo establecido entre sesiones	No

Tabla 3.1: Resumen de las bases de datos utilizadas.

3.2 Algoritmos de reconocimiento

En este apartado se resumen el proceso de extracción de características sobre los trazos táctiles. Asimismo, se citan y se describen los dos algoritmos de reconocimiento empleados en el trabajo realizado.

3.2.1 Parametrización de trazos táctiles

Como se explicaba en la figura 1.1, existe una arquitectura común en los sistemas de autenticación en dispositivos móviles.

Dentro de la parametrización de los trazos táctiles, en primer lugar, se adquieren los datos de los usuarios a partir de los trazos realizados sobre la pantalla táctil de los dispositivos. Sobre cada punto del trazo adquirido, se obtienen las coordenadas *x* e *y*, la presión ejercida, el *timestamp*, entre muchos otros.

A continuación, se agrupan las secuencias de puntos almacenados en grupos o trazos, eliminando los de menor tamaño de cara a ofrecer mayor robustez al sistema.

Finalmente, cada trazo queda descrito por un vector de características. Entre este conjunto de características se encuentras la velocidad, la aceleración, el ángulo, la longitud, etc. La figura 2.1 muestra un ejemplo de características extraídas de un trazo en concreto.

3.2.2 Máquinas de vectores de soporte

Las máquinas de vectores de soporte (SVM) son un conjunto de algoritmos de aprendizaje supervisado pertenecientes a la familia de los clasificadores lineales. Se aplican en problemas de clasificación y regresión.

El objetivo consiste en tratar de independizar un conjunto de dos clases a dos espacios diferentes mediante un hiperplano. Existen un número infinitos de hiperplanos que realicen la separación indicada, pero la solución óptima para obtener una clasificación correcta radica en obtener el mayor margen posible entre los elementos de las categorías disponibles. El margen mencionado es la distancia mínima entre el hiperplano y cada una de estas clases [6].

Concretamente, el kernel SVM utilizado en este trabajo ha sido Radial Basis Function (RBF). Este tipo de kernel queda descrito en la siguiente fórmula, donde x y x' son dos muestras, y σ es un parámetro libre, correspondiéndose con la desviación estándar del kernel gaussiano.

$$K(x, x') = e^{(-\frac{||x-x\prime||^2}{2\sigma^2})}$$

3.2.3 Modelo de mezclas gaussianas

Este algoritmo es un modelo probabilístico, también clasificado dentro de los algoritmos de aprendizaje supervisado, cuyo objetivo consiste en representar subpoblaciones de distribución normal dentro de una población generalista.

El conjunto de datos existentes sigue la distribución de un modelo mixto donde se haya más de un único pico en la distribución de estos. Por lo tanto, es multimodal, pudiéndose representar mediante una combinación de distribuciones unimodales, como se puede comprobar en la figura 3.1.

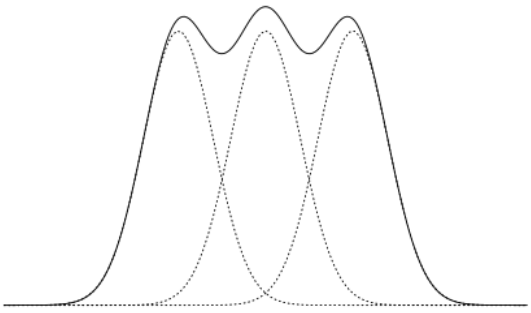

Figura 3.1: Ejemplo de modelo de mezclas gaussianas.

Un modelo de mezclas gaussianas se parametriza mediante dos tipos de valores. El primero de ellos consiste en el conjunto media "μ" y varianza "σ" de cada distribución gaussiana unimodal.

El segundo se basa en los pesos asociados "*w*" a cada distribución anterior. En la siguiente ecuación [16] se refleja la suma de *K* componentes gaussianos $\mathcal{N}$ definidos previamente.

$$p(x) = \sum_{i=1}^{K} w_i \mathcal{N}(x \mid \mu_i, \sigma_i)$$

Si se conoce el número de componentes que posee la distribución, se pueden estimar los parámetros previamente comentados mediante la técnica conocida como *Expectation Maximization (EM)*. Este método está formado por dos fases. En la primera, denominada *E step*, se calcula la expectación de los componentes citados. Finalmente, en la fase *M step*, se actualizan dichos componentes. El proceso se repite hasta que el algoritmo converja, como se confirma en la figura 3.2. En esta figura se contempla un ajuste progresivo de los valores peso, media y varianza de cada distribución normal, obteniendo así un resultado mayormente preciso.

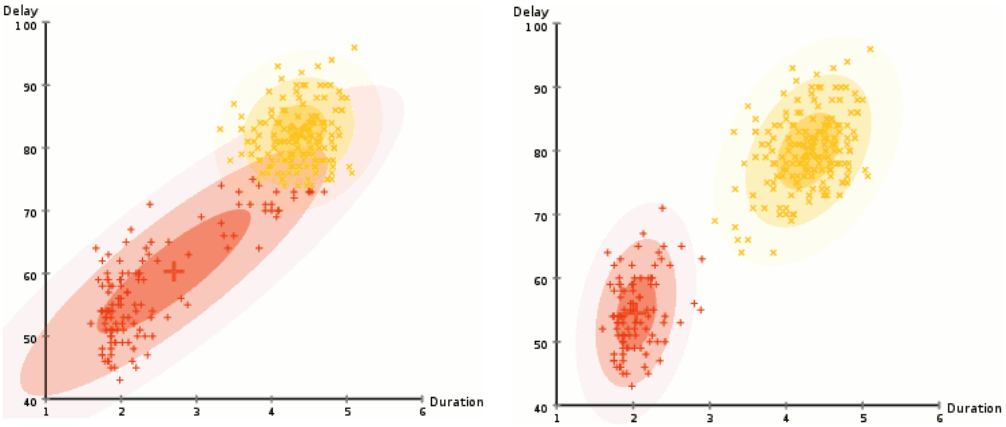

Figura 3.2: Representación del algoritmo EM. Figura de la izquierda estado inicial. Figura de la derecha estado final después de varias iteraciones. Fuente: [16].

Por otra parte, se ha hecho uso del modelo Universal Background Model (UBM) para obtener la distribución final. Este modelo es un GMM general entrenado por vectores de características de diferentes usuarios [6].

3.3 Autenticación continua

En esta sección se describe detalladamente el algoritmo de autenticación continúa empleado en este trabajo. Además, se citan dos variantes de este algoritmo, focalizándose en una y proveyendo las fórmulas correspondientes, así como ejemplos de resultados en forma de gráfica.

3.3.1 Quickest Change Detection

Este algoritmo, propuesto en [17] y aplicado a biometría en [1], tiene como finalidad detectar el punto de cambio con el mínimo retardo posible (ADD) mientras se mantiene una pequeña probabilidad de falsa detección (PFD).

A continuación, se muestran las fórmulas que describen las variables ADD y PFD, dos conceptos previamente explicados en la sección 2.1.5.

$$ADD(\tau) = E[(\tau - T)^+]$$

$$PFD(\tau) = P[(\tau < T)]$$

Las dos ecuaciones están definidas para un instante τ, donde el instante de cambio de un usuario verídico a un impostor se indica mediante la letra T. $E[.]$ y $P[.]$ corresponden el promedio y la probabilidad con respecto a τ, respectivamente y $[(x)^+]$ la parte positiva de x.

En la primera fórmula se visualiza el promedio de tiempos transcurridos desde el momento actual hasta el instante de cambio. Por otra parte, la segunda ecuación evalúa la probabilidad de que se detecte al usuario verídico como impostor antes de que suceda el cambio.

Como se puede comprobar, existe cierta correlación entre las dos fórmulas mencionadas. Si se desea obtener un sistema donde el grado de precisión en la decisión sea relativamente alto, es decir, una probabilidad de falsa detección baja, se podrá lograr a costa de alcanzar un tiempo de detección de intruso elevado. Por lo tanto, para comparar el rendimiento de diferentes sistemas, se decide obtener un gráfico PFD-ADD, como el representado en la figura 3.3. Esta gráfica es de gran utilidad para el diseño del sistema final en función de los valores finales deseados. Se indica, mediante un color verde, la sección óptima donde se obtendrán los valores mínimos respecto a PFD-ADD.

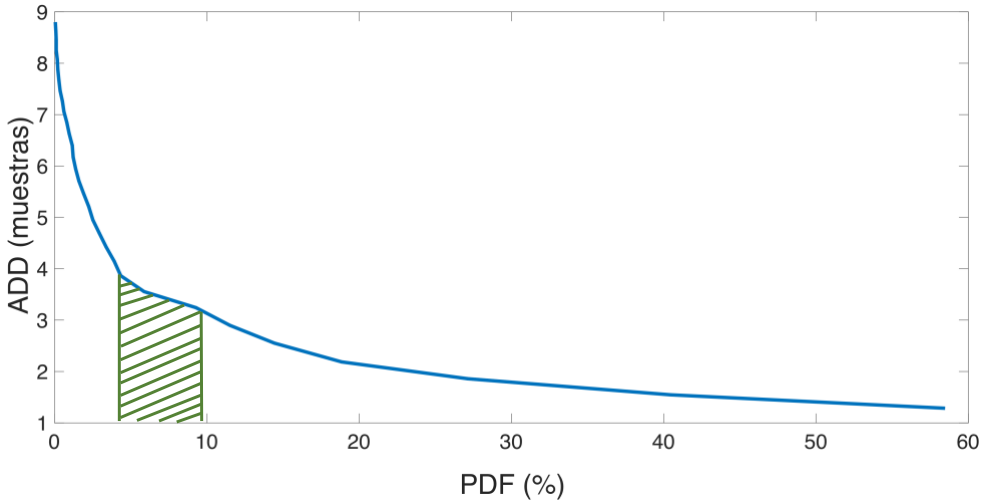

Figura 3.3: Curva PFD-ADD.

En [1] se citan dos tipos de algoritmos QCD. Comúnmente a los dos métodos, se definen previamente dos distribuciones.

La primera de ellas, denominada distribución pre-cambio (f_0), consiste en la observación obtenida antes del cambio de usuario genuino a impostor. La segunda, apodada como distribución post-cambio f_1, radica en la observación a posteriori.

Los dos algoritmos se enumeran a continuación:

- **Bayesian QCD (BQCD):** en este algoritmo se asume que el tiempo del instante de cambio T, comentado previamente, se corresponde a una distribución geométrica, definiéndose previamente la probabilidad de que aparezca el intruso en el contexto. Gracias a dicha teoría, se puede optimizar el sistema propuesto redefiniendo las fórmulas correspondientes a los valores ADD y PFD. El objetivo final consiste en minimizar el primer valor aludido manteniendo constante el segundo.

- **MiniMax QCD (MQCD):** este método se formula debido a que en la mayoría de sistema de autenticación continua no se conoce la probabilidad de intrusión a priori. Por lo tanto, el punto de cambio τ se considera un valor indeterminado. El objetivo de este procedimiento coincide con el de BQCD. La solución óptima se obtiene utilizando el algoritmo CumSum.

Para desarrollar los algoritmos, se definen en dicho documento un procedimiento focalizado en dos fases:

- **Fase 1 o fase de entrenamiento:** en esta fase se obtienen las distribuciones f_0 y f_1 mediante los datos provenientes de la ejecución previa de tareas en los smartphones por parte de los usuarios.

- **Fase 2 o fase de pruebas:** en esta etapa, para tomar las decisiones oportunas respecto a la verificación del usuario, se tiene en cuenta la secuencia de observaciones pasadas, además de las distribuciones f_0 y f_1 .

En la fase 2, se calcula el cociente de verosimilitud o *likelihood ratio*, detallada en la siguiente ecuación:

$$Likelihood\ ratio = \log(\frac{f_1(x_n)}{f_0(x_n)})$$

Concretamente, cuando se produce el instante de cambio T, es decir, pasar de usuario genuino a impostor, el valor obtenido por la fórmula descrita tiende a infinito. Por consiguiente, el valor descrito también crece si el usuario genuino presenta variaciones en su rostro. Por el contrario, este valor decrece si el rostro del usuario genuino vuelve a la expresión natural inicial.

En este Trabajo de Fin de Máster se ha desarrollado el algoritmo MQCD. En este procedimiento se define la variable *Score*, inicializándose a cero para posteriormente crecer o decrecer en función de los datos adquiridos. También se define un umbral, el cual es un valor establecido previamente para detectar si un usuario es impostor o no.

El procedimiento se fundamenta en los siguientes pasos:

Paso 1: En primer lugar, se debe inicializar la variable Score a 0.

Paso 2: Posteriormente, se incrementa el valor de Score sumando a este el valor obtenido por la ecuación Likelihood ratio, como se puede visualizar en la siguiente fórmula.

$$Score = Score + Likelihood\ ratio$$

Paso 3: Una vez calculado dicho resultado, se iguala a 0 el dato resultante de Score solo si este es negativo.

Paso 4: Se comprueba si dicho valor supera un umbral preestablecido. Si se rebasa este umbral, el usuario será detectado como intruso y se procederá a bloquear el dispositivo utilizado. Si no se produce este caso, se obtiene un nuevo Score proveniente de una nueva muestra del usuario y se repite todo el procedimiento desde el paso 2.

A continuación, en la figura 3.4 se muestra el resultado del algoritmo MQCD sobre un usuario en concreto. Para obtener dicha gráfica, se han utilizado un total de 16 muestras genuinas o trazos realizados con el dedo y parametrizados de dicho usuario concatenadas con el mismo número de muestras de un usuario impostor. Respecto al umbral, se ha establecido un valor igual a 4.

Como se puede ver, existe un pico sobre la muestra número 4 producido por desigualdades entre los datos de entrenamiento y la información del usuario verídico en ese instante. En este caso, el usuario no sería detectado como impostor debido a que el pico mencionado no es lo suficientemente grande como para sobrepasar dicho umbral.

Posteriormente, se comprueba como el valor ofrecido por el algoritmo implicado empieza a ascender hasta sobrepasar el umbral. En el momento que el resultado obtenido sobrepase esta variable, el usuario será catalogado como impostor. Finalmente, presenta una serie de caídas, sin volver a sobrepasar el umbral, manteniendo una tendencia ascendente.

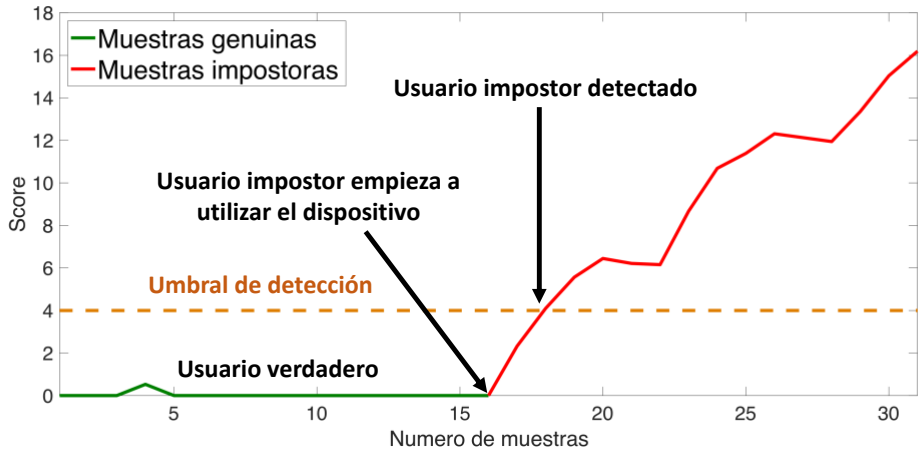

Figura 3.4: Resultado del algoritmo MQCD del usuario número nº4 de la base de datos Serwadda.

Seguidamente, en la figura 3.5 se exponen más ejemplos de resultados provenientes del algoritmo MQCD en otros usuarios. En estas gráficas se puede comprobar también que, a pesar de obtener ciertos picos o valores relativamente altos en muestras genuinas, se puede establecer un umbral determinado que alcance la detección de impostores.

Dentro de esta figura, el algoritmo funciona perfectamente sobre las muestras genuinas de la gráfica 3.5. a), ya que el resultado se mantiene a cero de manera constante y sin presentar ningún posible pico que pueda superar el umbral. Sin embargo, dentro de las muestras impostoras, el resultado tarda un cierto número de estas en incrementarse. Por lo tanto, en este caso, el algoritmo ha actuado de manera permisiva respecto a la detección de intrusos.

El suceso previo no ocurre en las demás gráficas. En estas, el valor devuelto por el algoritmo se incrementa en el instante donde se empiezan a incluir muestras impostoras. Además, a diferencia de la primera gráfica comentada, presentan varios picos dentro de los resultados sobre las muestras genuinas. Al seleccionar un umbral en estos casos, esta serie de crestas no serían un problema ya que no son lo suficientemente elevadas como para catalogar al usuario verdadero como impostor.

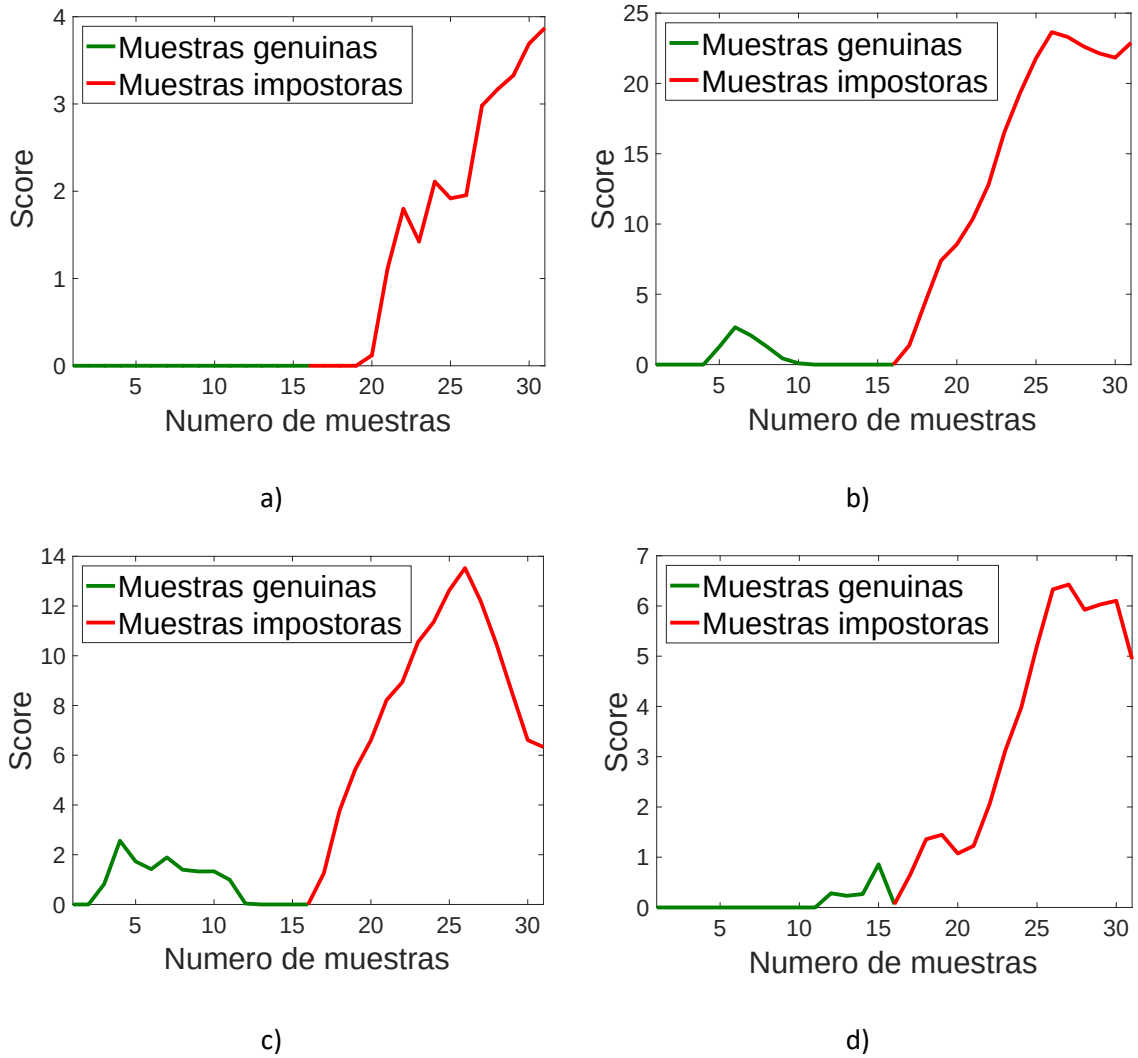

Figura 3.5: Resultado del algoritmo MQCD de varios usuarios. a) Usuario nº1, base de datos Serwadda, trazo tipo down. b) Usuario nº20, base de datos Serwadda, trazo tipo up. c) Usuario nº20, base de datos Serwadda, trazo tipo left. d) Usuario nº6, base de datos UMDAA-02, trazo tipo left.

3.4 Protocolo de evaluación

En esta sección se explican los procedimientos seguidos para evaluar los algoritmos desarrollados.

Los datos referentes a las bases de datos utilizadas se separan principalmente en dos bloques. El primer bloque corresponde a los datos intra-session. Esta agrupación está formada por comparaciones de datos obtenidos en periodos relativamente cercanos, por ejemplo, en el mismo día. El segundo corresponde a inter-session. En este caso, este bloque está formado por comparaciones de datos adquiridos en periodos más lejanos, siendo habitualmente la diferencia mayor que un día. Cómo se indicaba en la figura 2.6, dentro de cada bloque se distinguen un total de 4 particiones según el tipo de movimiento del trazo realizado. Estas particiones se corresponden con Down, Left, Right y Up.

De cara a obtener los resultados finales, es necesario extraer una serie de conclusiones previas. Todos los resultados se obtienen para cada algoritmo explicado en la sección 3.2 y, además,

para la fusión de estos. Esta fusión consiste en promediar los valores obtenidos por cada algoritmo empleado [6][4][2].

Primeramente, se adquieren las muestras genuinas e impostoras de cada usuario en función del umbral empleado. Con el objetivo preferente de calcular los *Equal Error Rate* (EER) del sistema, se obtienen las gráficas FAR-FRR. En la figura 3.6 se puede contemplar un esquema de este hecho.

Una vez se han obtenido los EER correspondientes, se procede a compararlos de diferentes modos. En primer lugar, se diferencian los datos equiparados en función de la posición del dispositivo, es decir, si está en modo landscape o portrait, el tipo de sesión, el trazo realizado y el modelo de base de datos. Los métodos empleados quedan descritos a continuación:

- **Experimentos globales:** se obtienen una serie de tablas donde quedan reflejadas comparaciones a nivel global de todos los usuarios.

- **Mejores y peores usuarios:** en este experimento, se procede a comparar los usuarios que alcanzan las mejores puntuaciones por un lado y los que obtienen las peores por otro. Posteriormente, se realizan búsquedas de patrones de coincidencia entre usuarios inter-session e intra-session mediante la exposición de estos en un mismo gráfico, ordenando los datos de mayor a menor en función de las puntuaciones adquiridas. Por otra parte, se calculan mapas de calor sobre las listas obtenidas de cara a alcanzar mayores conclusiones.

Una vez obtenidos los EER sobre los datos de los usuarios, se procede a calcular el conjunto de curvas PFD-ADD provenientes de la aplicación del algoritmo QCD. Como se puede comprobar en las figuras 3.4 y 3.5, estableciendo umbral se determinará cuando el dispositivo debe ser bloqueado si algún valor procedente del algoritmo supera este límite.

Para obtener las curvas mencionas, se evalúan en primer lugar PFD y ADD por separado, en función del umbral utilizado. Este procedimiento se puede visualizar en los ejemplos mostrados en la figura 3.7. En la sección 4 se explicarán de manera más exhaustiva el comportamiento de estos resultados.

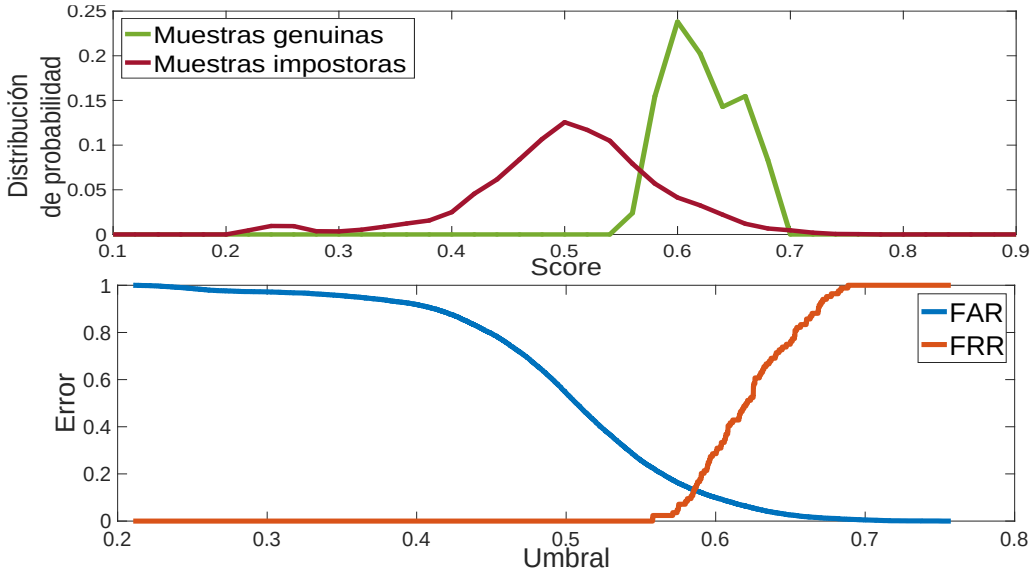

Figura 3.6: Distribución de probabilidad de muestras genuinas vs impostoras y curvas FAR-FRR de un usuario específico.

Una vez se han obtenidos los valores correspondientes a las gráficas mencionadas previamente, se procede a combinarlas calculando las curvas PFD-ADD. Este resultado está visible en la figura 3.3. Además, se estiman los usuarios impostores que nunca llegaron a sobrepasar el umbral preestablecido en todos los experimentos. Está información se presentan en función del umbral, ADD y PFD.

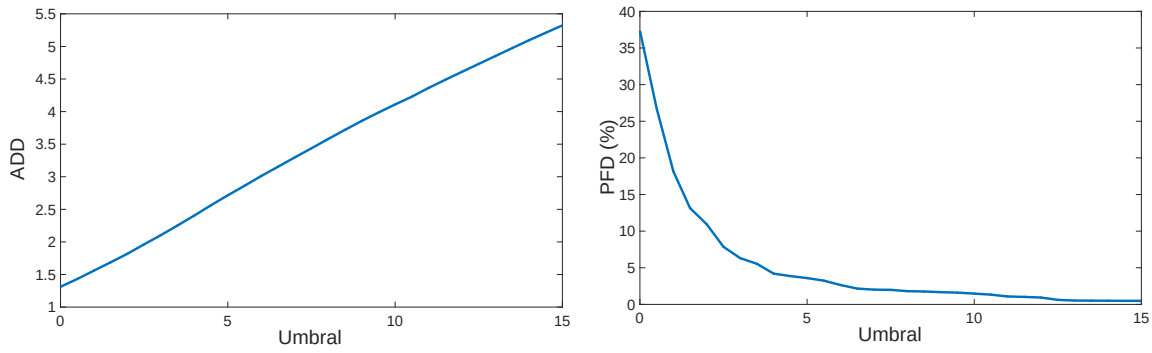

Figura 3.7: Curvas ADD y PFD en función del umbral.

En relación al número de muestras empleadas en los experimentos, en las bases de datos Serwadda y Frank se utilizaron en cada usuario un total de 30 trazos para entrenamiento y el resto disponible para test. por cada 3 muestras genuinas, se incluyen 10 impostoras dado su mayor número disponible.

En la base de datos UMDAA-02, al no haber datos clasificados en inter-session e intra-session y de cara a poder ofrecer comparaciones entre los distintos EER obtenidos, la división de datos en entrenamiento y test se realiza de forma diferente. Este procedimiento se puede visualizar en la figura 3.8.

En primer lugar, se obtiene por cada usuario un 70 % de las muestras totales. Sobre ese porcentaje, se dedica un total del 70% de muestras para entrenamiento y el 30% restante para pruebas, denominándose estas muestras de desarrollo. Una vez obtenidos los EER correspondientes, en este caso EER_1 en la figura, se procede a ejecutar de nuevo dicha división entrenamiento-test sobre el 100% de los casos, para así calcular EER_2. En este nuevo fraccionamiento, las muestras de desarrollo previas se incluyen en el conjunto de entrenamiento final.

El objetivo de este método radica en comprobar si los resultados obtenidos para una proporción inicial de usuarios presentan un grado de igualdad o similitud respecto al total de las muestras adquiridas, es decir, si los resultados son persistentes y uniformes en el tiempo.

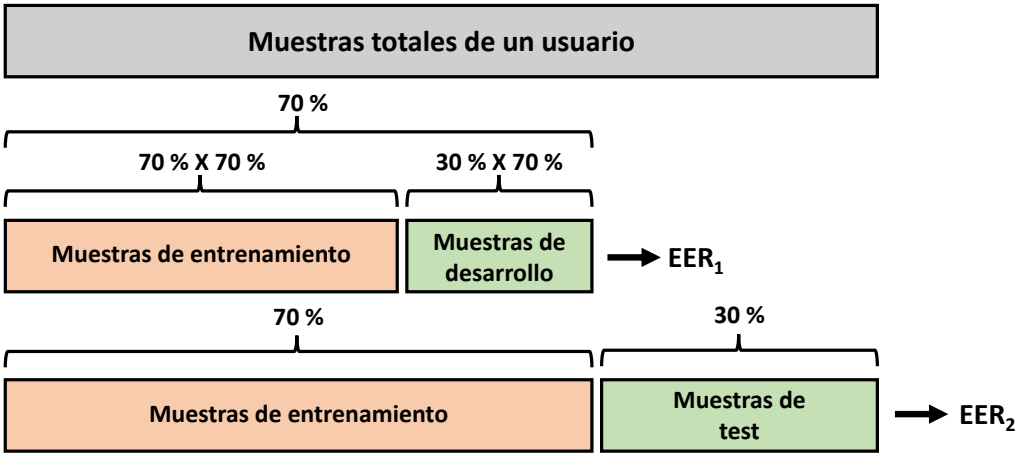

Figura 3.8: División de datos de la base UMDAA-02 para los experimentos realizados.

4 Resultados experimentales

En esta sección se visualizan e interpretan los resultados obtenidos por los métodos desarrollados en la sección 3.4. Asimismo, Este bloque está compuesto por un conjunto de 3 subapartados, los cuales se citan a continuación.

4.1 Baseline

En dicho apartado se introducen los resultados provenientes del punto de partida [6]. Se añaden los resultados de la nueva base de datos analizada [10]. Estos valores se corresponden con los EER obtenidos para el conjunto de usuarios examinados.

En la tabla 4.1 se procede a comparar los EER promedio entre usuarios a través de las bases de datos Serwadda y Frank. Al no disponer de suficientes muestras en modo landscape de Frank, solo se comparan en modo portrait. Lo mismo ocurre para los trazos tipo Up de esta base de datos.

Los datos incluidos se diferencian en el tipo de trazo, el tipo de comparación o el algoritmo empleado.

Bases de datos	Algoritmos	Intra-session				Inter-session			
		Down	Left	Right	Up	Down	Left	Right	Up
Serwadda	Fusión	7.99	5.26	5.39	7.38	15.98	15.54	17.14	17.76
	UBM	17.52	12.69	13.45	17.32	21.65	19.43	21.87	23.75
	SVM	10.19	6.94	7.31	8.57	22.02	23.65	24.73	23.12
Frank	Fusión	7.28	5.56	5.60		10.74	9.65	9.48	
	UBM	16.48	12.63	11.17		14.44	18.49	19.61	
	SVM	8.93	5.82	7.16		15.32	9.96	7.84	

Tabla 4.1: Comparación EER promedios, modo portrait, bases de datos Serwadda y Frank.

En esta tabla se puede ver cómo en la fusión, al combinar los datos obtenidos por los métodos UBM y SVM, se obtiene resultados mucho más óptimos, tal y como se comentaba en [2]. Por otra parte, se alcanzan mejores resultados en comparaciones intra-session. Esto es debido a que los resultados de dichas comparaciones son más cercanos al tiempo, por lo tanto, más equivalente entre sí. Cabe destacar como los trazos tipo Left y Right adquieren un mayor rendimiento en la mayoría de casos analizados, en comparación con Up y Down. Esto puede deberse a la costumbre que posee un usuario al realizar movimientos y gestos en horizontal de manera rutinaria, en vez de llevarlos a cabo en vertical.

A continuación, se exponen los datos referentes a la base de datos UMDAA-02. Se ha procedido a separarlos en una tabla diferente ya que, como se comentó previamente, no comparte el mismo método de comparación inter e intra-session.

Concretamente, para uniformar el conjunto de datos evaluados, y como las demás bases promedian los resultados que se han ido obteniendo con una ventana de tamaño igual a 10, los datos de las tablas 4.2 y 4.3 han sido calculados con un valor de W_{swipes} igual al anterior.

En las dos tablas comentadas, se puede comprobar como los valores permanecen más o menos constantes si comparamos los datos totales con la fracción de estos. Esto demuestra que los datos no varían de forma brusca a medida que el pasa el tiempo.

Si se estudian detenidamente, se contemplan una serie de irregularidades entre los trazos tipo right en portrait desarrollo y portrait test. Asimismo, también se visualizan en los trazos de tipo up en landscape desarrollo y landscape test. Esto se debe a casos localizados de usuarios que presentan este tipo de trazos de forma irregular y, por lo tanto, corrompen la media, pero si se contemplan los otros tipos de trazos, la homogeneidad descrita sigue presente.

Comparando los modos portrait y landscape de este caso, el primer modo ofrecer mayor homogeneidad debido a la facilidad que presenta al usuario realizar gestos con dicha posición.

Base de datos	**Algoritmos**	**Portrait desarrollo**				**Portrait test**			
		Down	Left	Right	Up	Down	Left	Right	Up
UMDAA-02	Fusión	14.47	16.65	22.46	15.64	14.39	17.98	16	15.33
	UBM	20.63	28.28	32.89	26.99	23.26	28.18	26.20	23.81
	SVM	16.37	17.12	22.11	16.90	14.09	17.08	17.88	15.98

Tabla 4.2: Comparación EER promedios, modo portrait, base de datos, UMDAA-02, tamaño de ventana = 10.

Base de datos	**Algoritmos**	**Landscape desarrollo**				**Landscape test**			
		Down	Left	Right	Up	Down	Left	Right	Up
UMDAA-02	Fusión	20.10	17.25	17.36	19.07	20.53	16.66	14.67	11.94
	UBM	25.11	22.24	25.96	26.62	31.15	25.85	26.07	18.17
	SVM	20.72	21.18	19.19	23.23	18.31	13.68	14.19	18.63

Tabla 4.3: Comparación EER promedios, modo landscape, base de datos UMDAA-02 tamaño de ventana = 10.

4.2 Autenticación continua

En este apartado se analizan los resultados ofrecidos por el algoritmo MQCD sobre las diferentes bases de datos utilizadas.

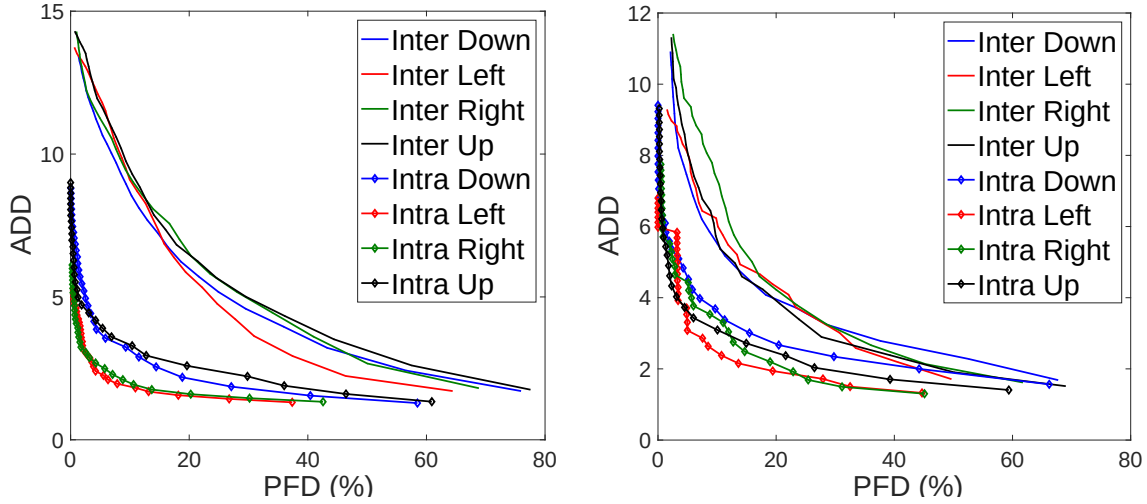

Figura 4.1: Comparaciones curvas PFD-ADD, base de datos Serwadda. a) Modo portrait. b) Modo landscape.

En la figura 4.1 se puede comprobar como los resultados obtenidos sobre las comparaciones de datos en una única sesión, correspondiente con las curvas tipo intra-session, ofrecen un rendimiento más óptimo en comparación con los resultados obtenidos sobre las comparaciones de los datos en dos sesiones diferentes, siendo estas las curvas tipo Inter. Esto se debe a la mayor semejanza de gestos producidos por el usuario en el dispositivo analizado en una única sesión en comparación con sesiones dispares.

En este suceso, obtener un resultado superior supone alcanzar un área menor bajo la curva analizada, ya que esto representa poder obtener una probabilidad de falsa detección reducida, a cambio de obtener un tiempo de retardo promedio no demasiado grande, y viceversa.

Por otra parte, se puede visualizar como entre diferentes movimientos en un mismo tipo de comparación, es decir entre Intra Down e Intra Left, o entre Inter Down e Inter Left, por ejemplo, no existe tanta diferencia en rendimiento como ocurría en el ejemplo analizado anteriormente. Este suceso demuestra que se podrá verificar al usuario con cualquier tipo de movimiento entre los descritos previamente, ya que ninguno prevalece de manera notoria sobre el resto.

Si se comparan las dos gráficas, no se aprecian grandes diferencias respecto a las características comentadas previamente. Sin embargo, los resultados en portrait son ligeramente mejores. Esto se debe a que los usuarios suelen estar más habituados a utilizar el móvil en esta posición en el día a día, como ya se comentó en resultados de otras secciones donde el suceso era el mismo.

A continuación, en la figura 4.2, se muestra otro ejemplo sobre la base de datos Frank. En este caso, las desigualdades comentadas previamente entre los gestos inter-session e intra-session son menos notorias, pero se siguen diferenciado claramente los dos bloques.

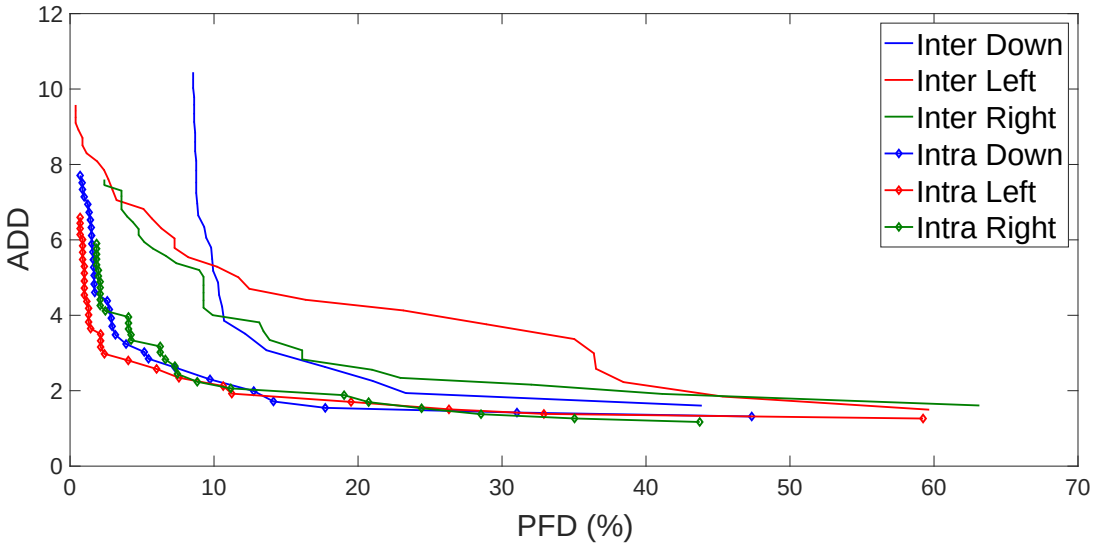

Figura 4.2: Comparaciones curvas PFD-ADD, base de datos Frank, modo portrait.

Finalmente, en la figura 4.3 se exponen las curvas PFD-ADD respectivas a la base de datos UMDAA-02. Los resultados calculados para el análisis parcial de los datos, es decir, el 70% de las muestras totales, reflejan un alto grado de similitud en comparación con el 100% de las muestras totales, a diferencia de las otras bases de datos analizadas. Por lo tanto, en este experimento se demuestra la línea continuista de los usuarios analizados a lo largo del tiempo.

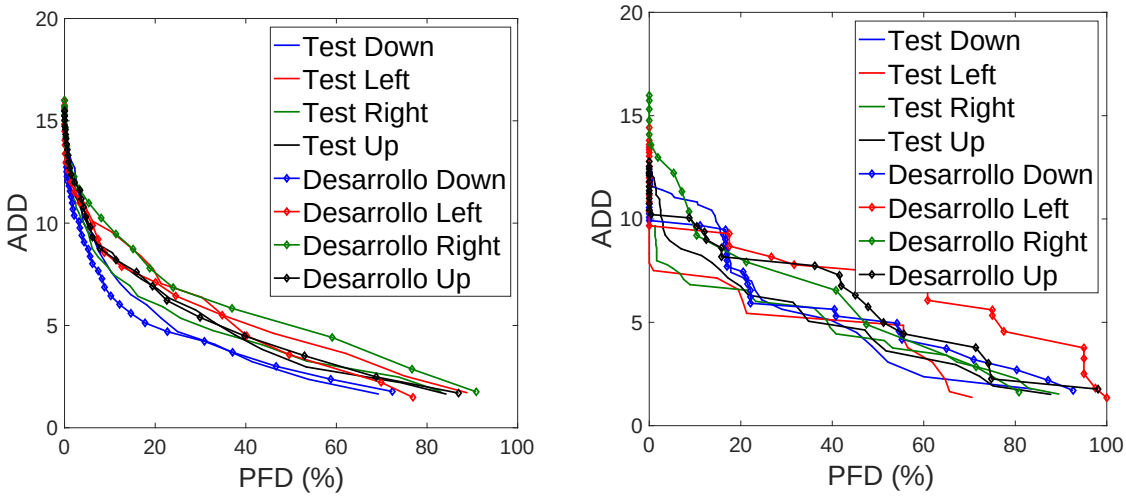

Figura 4.3: Comparaciones curvas PFD-ADD, base de datos UMDAA-02. a) Modo portrait. b) Modo landscape.

Seguidamente se analizan el porcentaje de usuarios impostores respecto al total que no llegaron a ser detectados por el algoritmo QCD. En la figura 4.4, se analiza este escenario en función del umbral preestablecido. Como se puede apreciar, el número de impostores localizados se incrementa a medida que el umbral se eleva. Esto es debido a que, aunque el impostor adquiera un resultado elevado, dicho valor no alcanzará un umbral cada vez mayor.

Con el fin de obtener una visión y un análisis más amplio, se procede a representar el porcentaje mencionado con respecto a las variables ADD y PFD, contempladas en la figura 4.5.

En el primer caso, el porcentaje aumenta a medida que aumenta el retardo de detección del intruso. En la segunda gráfica, ocurre todo lo contrario, ya que, si se requiere conseguir probabilidades de falsa detección reducidas, no habrá falsos positivos pero la detección de impostores será más difícil.

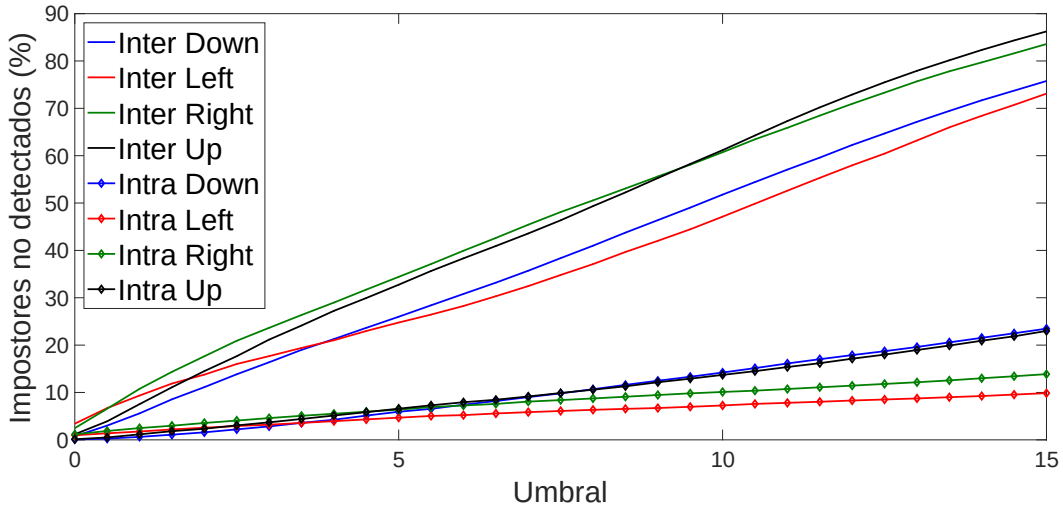

Figura 4.4: Usuarios impostores no detectados respecto al umbral, base de datos Serwadda, modo portrait.

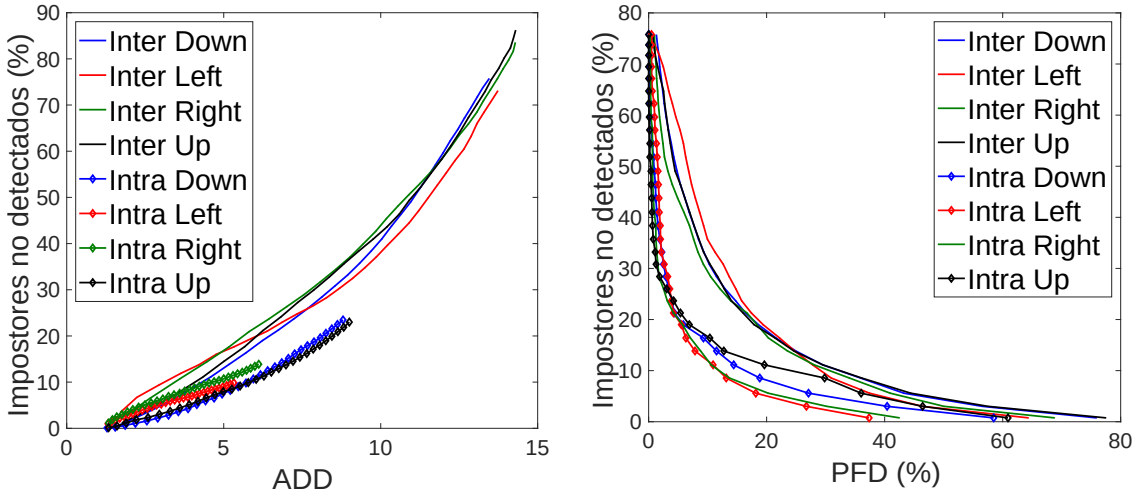

Figura 4.5: Usuarios impostores no detectados respecto a ADD y PFD, base de datos Serwadda, modo portrait.

En la figura 4.6 se muestran otros ejemplos referentes a las bases de datos Serwadda, en modo landscape y Frank en modo portrait. Se aprecia notablemente en landscape una mayor intersección de las sesiones inter e intra, en comparación con portrait, tanto de Serwadda como de Frank, donde se contemplaban claramente independientes.

Por otra parte, en las gráficas de porcentaje de impostores no detectados frente a ADD o PFD, la tendencia creciente y decreciente sigue siendo la misma que se analizó en la figura 4.5.

Respecto al grado de independencia entre sesiones inter e intra-session, se aprecia mayor aislamiento en las gráficas respecto a PFD.

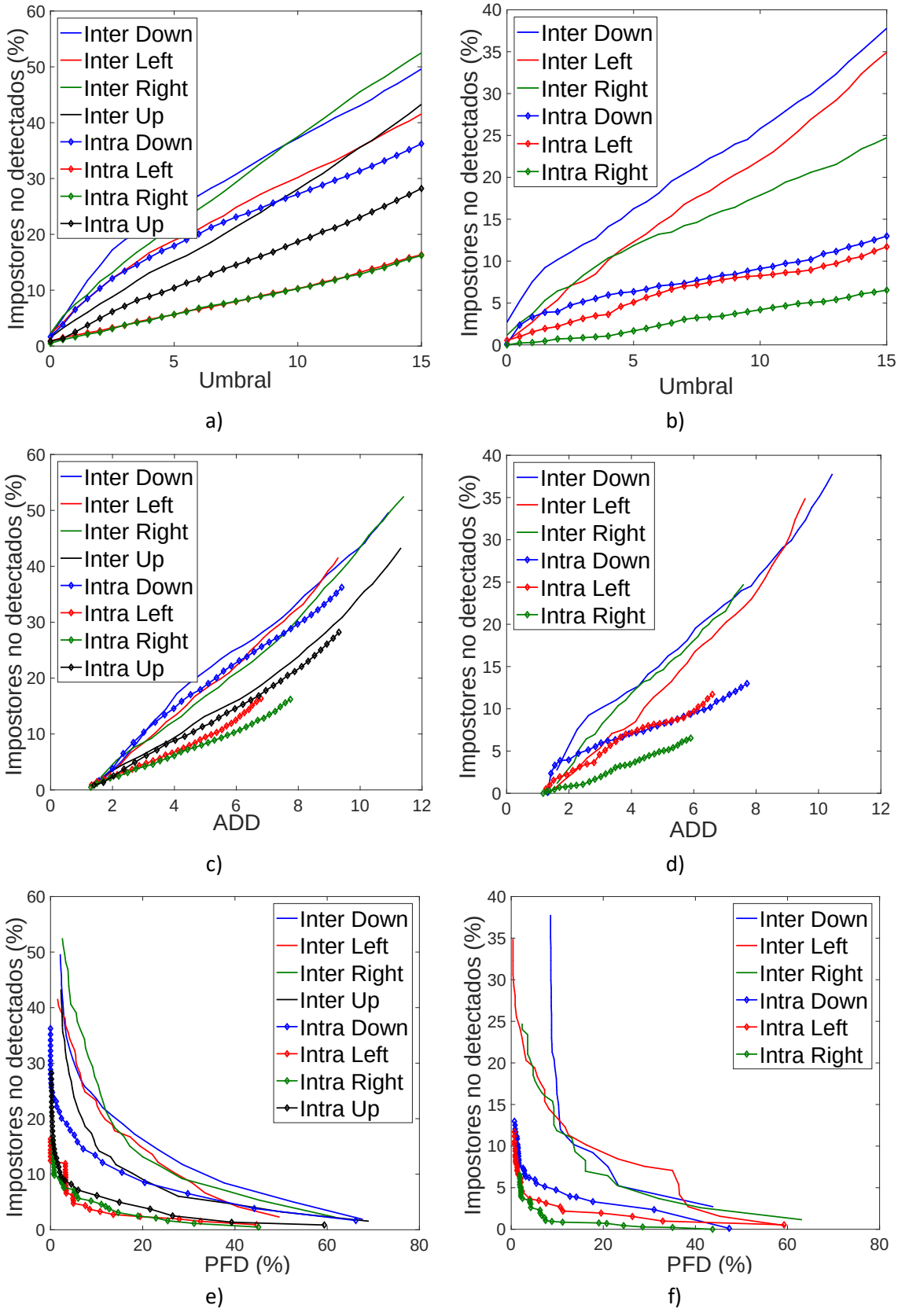

Figura 4.6: Usuarios impostores no detectados respecto al ADD y PFD. a) c) e) Base de datos Serwadda, modo landscape. b) d) f) Base de datos Frank, modo portrait.

A continuación, en la figura 4.7, se realiza el mismo estudio, pero sobre la base de datos UMDAA-02. Este caso difiere totalmente a los previos comentados anteriormente. La finalidad

buscada de este experimento consiste en mantener cierta coherencia entre el segmento inicial de datos analizados y el total. Esta correspondencia es mayor en el modo portrait ya que, como se puede ver, hay menor distancia entre las gráficas parciales y sus correspondientes totales.

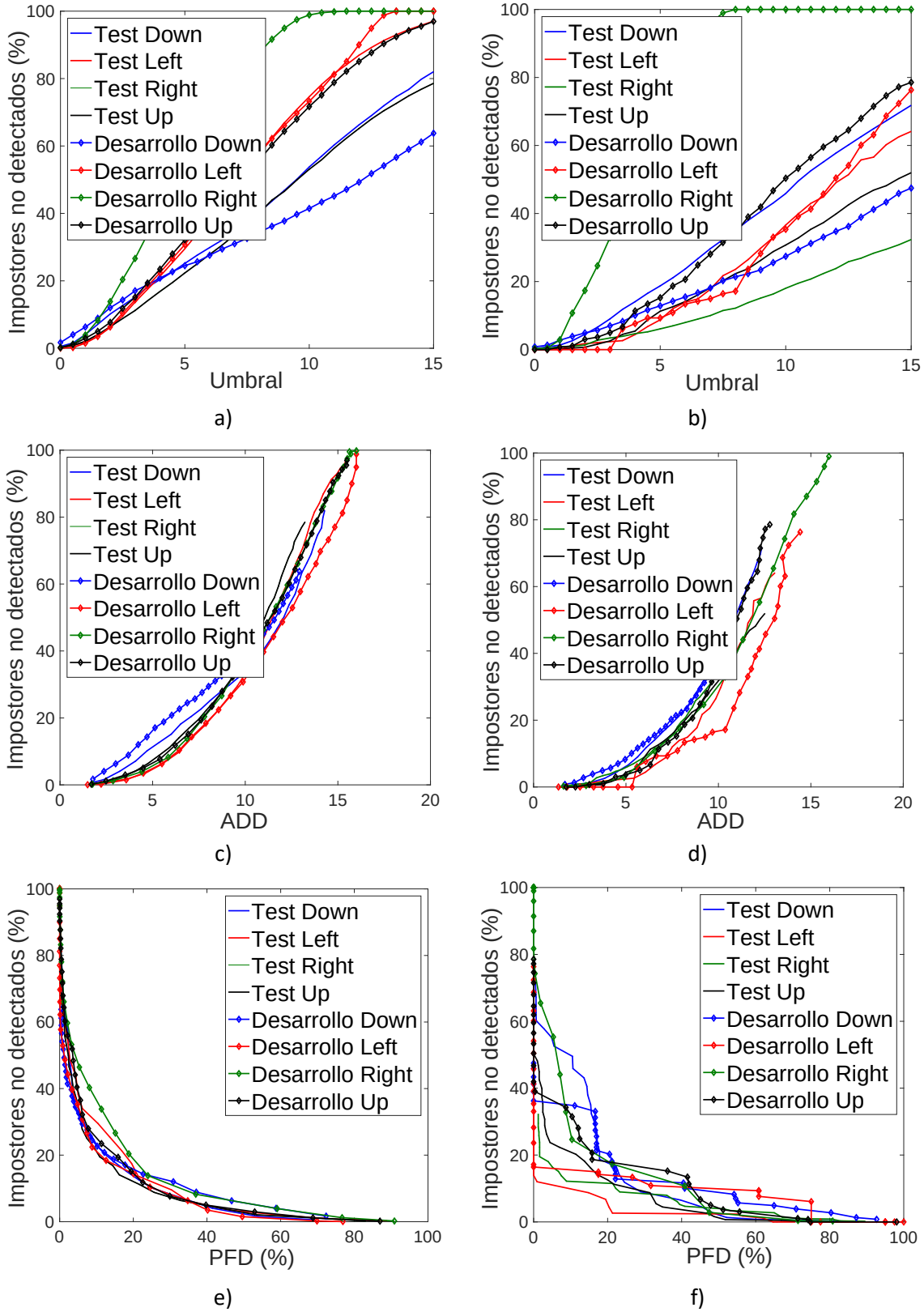

Figura 4.7: Usuarios impostores no detectados respecto al ADD y PFD, base de datos UMDAA-02. a) c) e) Modo portrait. b) d) f) Modo landscape.

4.3 Discusión de los resultados

A continuación, de cara a adquirir mayor criterio en la distinción entre usuarios, además de buscar patrones entre los datos obtenidos, se procede a ordenar los resultados pertenecientes a los usuarios, en función de si son mejores o peores entre sí.

El primer experimento consiste en ordenar los usuarios de mayor a menor puntuación con respecto a los EER calculados en sesión tipo intra-session. Una vez organizados, se obtiene para estos usuarios los valores EER referentes a la sesión tipo inter-session, como se muestra en la figura 4.8.

En las gráficas de esta figura, independientemente del tipo de trazo, se observa que los resultados EER tipo inter-session siguen un cierto aumento parecido a los resultados tipo intra-session, pero a diferencia de este, presenta múltiples altibajos.

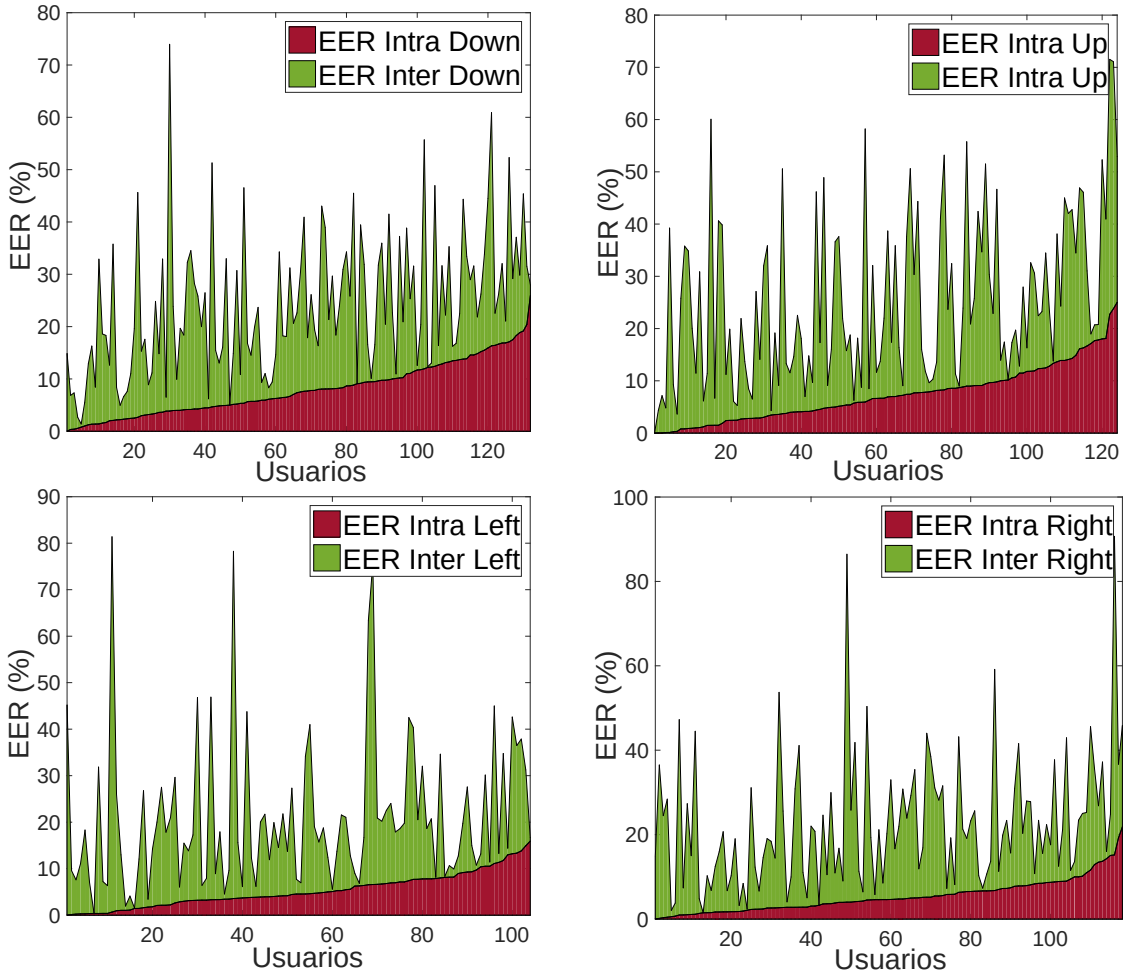

Figura 4.8: Usuarios ordenados por EER, intra-session, base de datos Serwadda, modo portrait.

En la figura 4.9 se ofrecen más ejemplos sobre las diferentes bases de datos. En estos casos, como se puede observar, al ser el número de usuarios menor, el número de picos ofrecidos por los resultados EER Inter Down son menores. Sin embargo, la tendencia ascendente se sigue sosteniendo como ocurre en la figura 4.8.

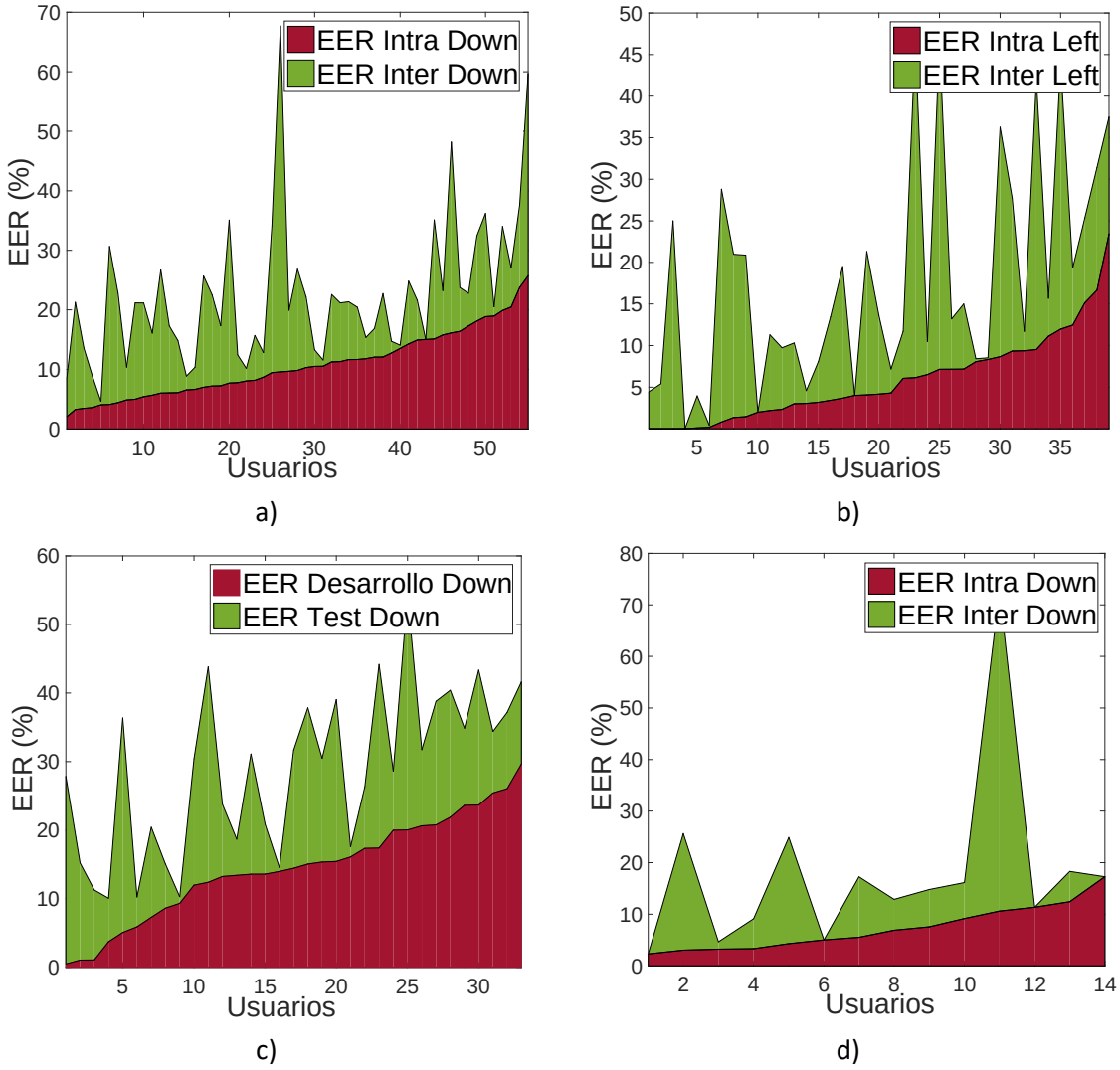

Figura 4.9: Usuarios ordenados por EER, intra-session.
a) b) Base de datos Serwadda, modo landscape. c) Base de datos UMDAA-02, modo portrait. d) Base de datos Frank, modo portrait.

A continuación, sobre los resultados previamente obtenidos, se selecciona un porcentaje de mejores y peores usuarios. Sobre dicha proporción, se realizan una serie de comprobaciones en función de cuantos usuarios de un tipo de trazo o tipo de comparación, entre los seleccionados previamente, se encuentran en otro tipo de trazo o comparación.

En la base de datos Serwadda existen de media 130 usuarios por tipo de trazo en modo portrait. Sobre este número se realiza una selección de 20 usuarios, es decir, aproximadamente un 15% del total. Este porcentaje también se aplica sobre el modo landscape de dicha base de datos, eligiendo un total de 8 usuarios sobre un promedio de 50 usuarios por tipo de trazo.

En UMDAA-02, al únicamente disponer de 30 usuarios por tipo trazo, se aplica un porcentaje mayor de selección, siendo este aproximadamente un 23%. Por lo tanto, el número de usuarios recopilados para este propósito es igual a 7.

En la figura 4.10 se han calculado una serie de mapas de calor. Estos mapas se corresponden con un conjunto de tablas previamente calculadas y disponibles en el anexo de este documento.

Como se puede comprobar, cada mapa de calor consta de 64 bloques ya que son una representación del conjunto de tablas mencionado anteriormente.

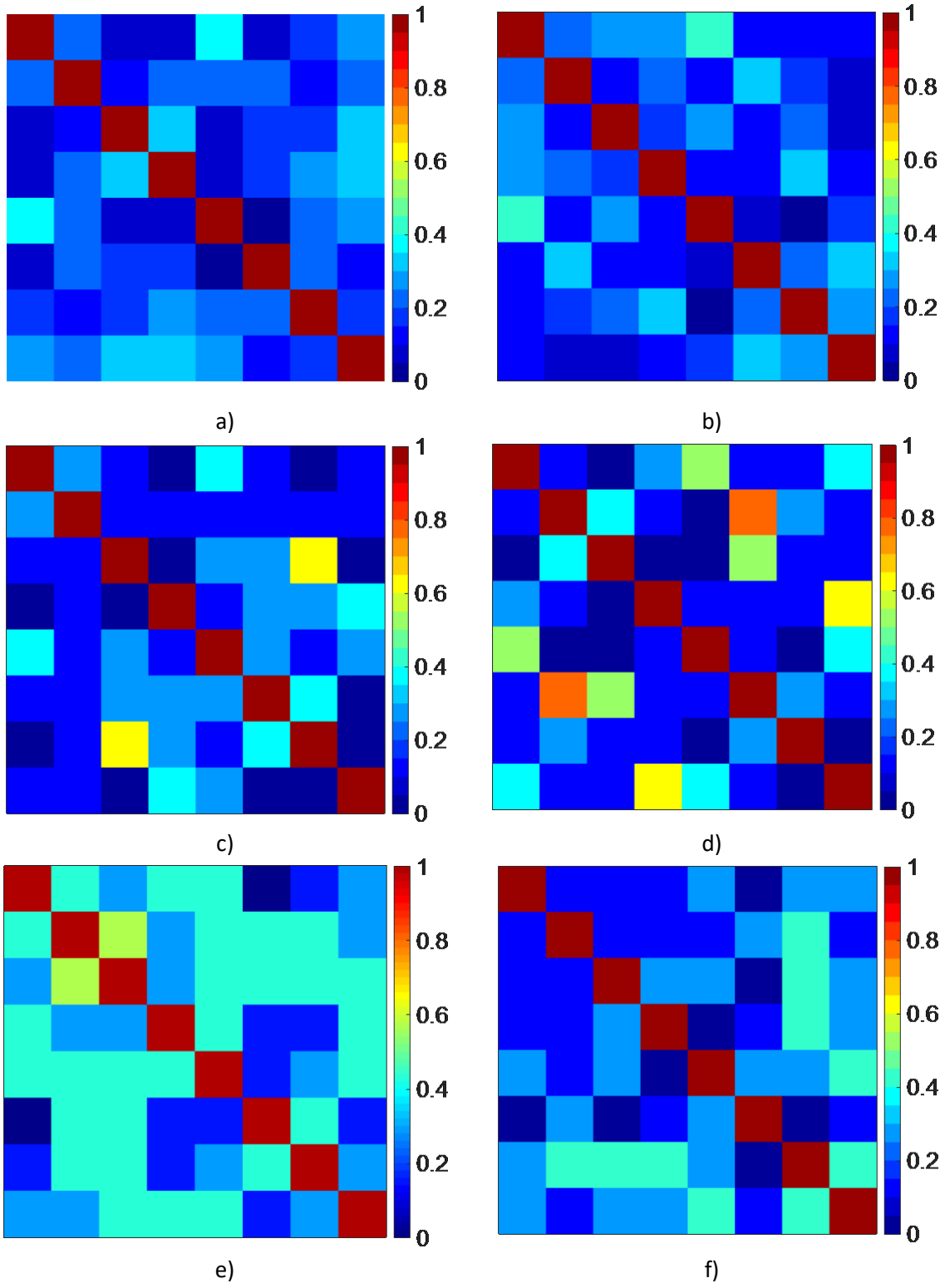

Figura 4.10: Mapa de calor porcentajes.
a) b) Mejores y peores usuarios, Base de datos Serwadda, modo portrait.
c) d) Mejores y peores usuarios, Base de datos Serwadda, modo landscape.
e) f) Mejores y peores usuarios, Base de datos UMDAA-02, modo portrait.

En las gráficas correspondientes a la base de datos Serwadda, se aprecia un alto porcentaje de coincidencias entre los trazos del mismo tipo pertenecientes a inter e intra-session. Cabe destacar que los resultados de las comparaciones en vertical son mejores que en horizontal. Por ejemplo, el porcentaje de coincidencia entre los tipos de trazos Down y entre up perteneciente a inter e intra-session es igual a 0.35 y 0.3 respectivamente.

En la figura 4.11 se analizan, dependiendo del tamaño de ventana utilizado para promediar los resultados finales, los EER promedios de desarrollo y test para cada tipo de trazo correspondientes a la base de datos UMDAA-02.

Como se puede visualizar, a medida que aumenta W_{swipes}, disminuyen los valores resultantes de los EER sustancialmente. En algunas zonas de las gráficas incluidas, los resultados empeoran puntualmente en un incremento de ventana, pero esto se subsana en siguientes aumentos de esta.

Por falta de tiempo y carga computacional, no se ha podido continuar los experimentos para un número de W_{swipes} mayor. En cualquier caso, los resultados tienden a estabilizarse a medida que se incrementa dicho valor.

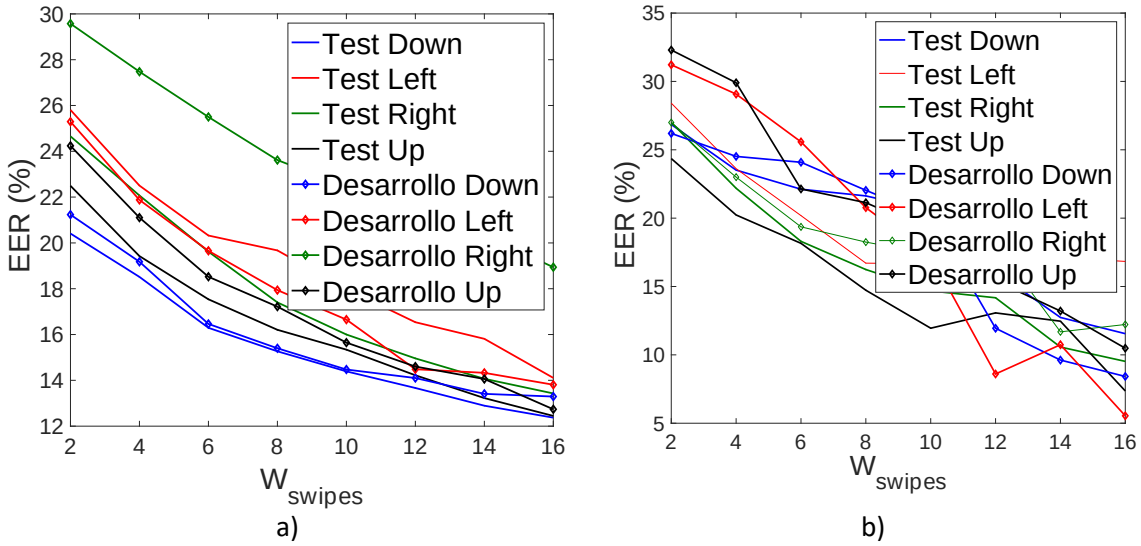

Figura 4.11: EER promedio en función de W_{swipes}, base de datos UMDAA-02.
a) Modo portrait. b) Modo landscape.

5 Conclusiones y trabajo futuro

5.1 Conclusiones

Durante la realización de este Trabajo de Fin de Máster se han realizado en primer lugar investigaciones sobre los diferentes trabajos científicos expuestos en el estado del arte. Gracias a estos documentos, se sentaron las bases acerca del reconocimiento biométrico mediante la interacción del usuario con pantallas táctiles. Además, a través del modelo de autenticación continua propuesto en [3], se ha realizado una extensión de [6] por medio del algoritmo QCD. Por otra parte, al conjunto de bases de datos ya analizadas se añadió una nueva propuesta por U. Mahbub en [10] para ampliar el estudio realizado y poder sacar un mayor número de conclusiones.

En la sección de resultados, se ha procedido a presentar los resultados ofrecidos en [6] de diferente modo de cara a contrastar la información proveniente de las sesiones inter e intra-session. Asimismo, se ha calculado el porcentaje de impostores respecto al total de usuarios que no son detectados por el sistema empleado. Este valor se muestra en función del umbral establecido, así como de las variables ADD y PFD. Se ha demostrado que la fusión alcanzada mediante la combinación de los resultados de UBM y SVM ofrece un mayor rendimiento. Además, las comparaciones intra-session obtienen resultados mejores que las comparaciones inter-session debido a la proximidad de sesiones en el primero.

Por otra parte, la manera en la que el usuario dispone del móvil en sus manos influye considerablemente en los resultados, ya que el modo portrait presenta mayor homogeneidad al ser la forma habitual con la que se sostiene un *smartphone*.

A continuación, se procedió a ordenar los usuarios por EER de mejor a peor resultado para un tipo de sesión, y se mostró para cada uno el valor correspondiente a la otra sesión realizada. Como se ha podido comprobar, existía un grado de similitud ascendente a medida que se desplaza en eje horizontal de dichas gráficas.

Para poder realizar un mayor número de comparaciones de manera general entre los resultados obtenidos, se han realizado una serie de tablas donde se reflejan los EER promedios en función del tipo de sesión y tipo de trazo. De igual modo, este conjunto se ha interpretado en forma de mapas de calor para mejorar visualmente las diferencias existentes entre unas comparaciones y otras. En estos mapas, se observan mejores resultados en comparaciones verticales, es decir, en trazos tipo down y up.

Finalmente, para la base de datos UMDAA-02 [10] se han calculados los EER promedios de cada tipo de trazo y sesión en función del tamaño de la ventana $W_{swipe.}$ Esta ventana se ha encargado de realizar la media de los valores incluidas en esta durante el cálculo de los resultados. Se ha concluido que, a mayor tamaño de ventana, se mejoran notablemente los EER resultantes hasta ir estabilizándose poco a poco estos valores.

5.2 Trabajo futuro

Tras la realización de este trabajo, aparecen varias líneas de trabajo futuro:

- Incluir un mayor número de bases de datos para afianzar las conclusiones obtenidas y alcanzar nuevas.
- Introducir nuevos métodos que permitan comparar de diferente forma los datos extraídos.
- Extender lo analizado y estudiado a otros métodos de reconocimiento biométrico, como pueden ser la localización del usuario gracias al GPS integrado en el dispositivo, o reconocimiento visual del rostro de este.
- Incrementar el número de sesiones realizadas. Actualmente, se han realizado dos sesiones. Se podrían incorporar un mayor número adquiriendo los datos en diferentes instantes del día, semana o mes, y poder catalogar cada uno por separado.
- Ampliar el número de gestos, siendo estos los 4 descrito durante el documento. Sería interesante de cara al estudio y al rendimiento del sistema incluir gestos de tipo rotatorio o diagonales.

Referencias

[1] P. Perera, and V. M. Patel, “Quickest intrusion detection in mobile active user authentication”, in Proc. Int. Conf. Biometrics Theory, Appl. Syst., pp. 1–8, September 2016.

[2] J. Fierrez, A. Pozo, M. Martinez-Diaz, J. Galbally, and A. Morales, “Benchmarking Touchscreen Biometrics for Mobile Authentication”, Information Forensics and Security IEEE Transactions on, vol. 13, pp. 2720 – 2733, May 2018.

[3] P. Perera and V. M. Patel, "Efficient and low latency detection of intruders in mobile active authentication", Information Forensics and Security IEEE Transactions on, vol. 13, pp. 1392-1405, 2018, ISSN 1556-6013.

[4] A. Pozo, J. Fierrez, M. Martinez-Diaz, J. Galbally and A. Morales, "Exploring a statistical method for touchscreen swipe biometrics", Proc. Int. Carnahan Conf. Secur. Technol. (ICCST), pp. 1-4, October 2017.

[5] M. Antal, Z. Bokor, and L. Z. Szabó, “Information revealed from scrolling interactions on mobile devices,” Pattern Recognition Letters, vol. 56, pp. 7–13, April 2015.

[6] A. P. Pérez, "Biometric authentication based on interaction with touchscreen", Trabajo Fin de Grado, Escuela Politécnica Superior, Universidad Autónoma de Madrid, May 2017.

[7] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, “Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication,” IEEE Transactions on Information Forensics and Security, vol. 8, no. 1, pp. 136–148, 2013.

[8] S. Theodoridis and K. Koutroumbas. “Pattern Recognition”, 4th ed. Academic Press, 2008.

[9] A. Serwadda, V. V. Phoha, and Z. Wang, “Which verifiers work?: A benchmark evaluation of touch-based authentication algorithms,” in Proc. IEEE BTAS, pp. 1–8, 2013.

[10] U. Mahbub, S. Sarkar, V. M. Patel, and R. Chellappa, “Active user authentication for smartphones: A challenge data set and benchmark results,” in Proc. IEEE BTAS, 2016.

[11] V. M. Patel, R. Chellappa, D. Chandra, and B. Barbello, “Continuous user authentication on mobile devices: Recent progress and remaining challenges,” IEEE Signal Processing Magazine, vol. 33, no. 4, pp. 49– 61, July 2016.

[12] H. Xu, Y. Zhou, and M. R. Lyu, “Towards continuous and passive authentication via touch biometrics: An experimental study on smartphones. In Symposium On Usable Privacy and Security”, SOUPS 2014, pp. 187–198, 2014.

[13] H. Zhang, V. M. Patel, M. Fathy, and R. Chellappa, “Touch gesture-based active user authentication using dictionaries,” in Proc. of the IEEE Winter Conference on Applications of Computer Vision, 2015, pp. 207–214.

[14] R. Kumar, V. V. Phoha, and A. Serwadda, “Continuous authentication of smartphone users by fusing typing swiping and phone movement patterns,” in Proc. IEEE BTAS, pp. 1–8, 2016.

[15] C. Shen, Y. Zhang, X. Guan, and R. A. Maxion, “Performance analysis of touch-interaction behavior for active smartphone authentication,” IEEE Transactions on Information Forensics and Security, vol. 11, no. 3, pp. 498 – 513, March 2016.

[16] J. McGonagle, V. Tembo, and A. Chumbley, "Gaussian Mixture Model", Brilliant.org, from https://brilliant.org/wiki/gaussian-mixture-model/, May 2018.

[17] V. V. Veeravalliand, and T. Banerjee, “Quickest Change Detection”, ArXiv e-prints, October 2012.

Glosario

API	Application Programming Interface

Anexos

		Intra-session				Inter-session			
		Down	**Left**	**Right**	**Up**	**Down**	**Left**	**Right**	**Up**
Intra-session	**Down**	1	0.2	0.05	0.05	0.35	0.05	0.15	0.25
	Left	0.2	1	0.1	0.2	0.2	0.2	0.1	0.2
	Right	0.05	0.1	1	0.3	0.05	0.15	0.15	0.3
	Up	0.05	0.2	0.3	1	0.05	0.15	0.25	0.3
Inter-session	**Down**	0.35	0.2	0.05	0.05	1	0	0.2	0.25
	Left	0.05	0.2	0.15	0.15	0	1	0.2	0.1
	Right	0.15	0.1	0.15	0.25	0.2	0.2	1	0.15
	Up	0.25	0.2	0.3	0.3	0.25	0.1	0.15	1

Tabla A.1: Porcentajes usuarios iguales en otros movimientos o comparaciones entre los mejores usuarios en función de sus EER, base de datos Serwadda, modo portrait.

		Intra-session				Inter-session			
		Down	**Left**	**Right**	**Up**	**Down**	**Left**	**Right**	**Up**
Intra-session	**Down**	1	0.2	0.25	0.25	0.4	0.1	0.1	0.1
	Left	0.2	1	0.1	0.2	0.1	0.3	0.15	0.05
	Right	0.25	0.1	1	0.15	0.25	0.1	0.2	0.05
	Up	0.25	0.2	0.15	1	0.1	0.1	0.3	0.1
Inter-session	**Down**	0.4	0.1	0.25	0.1	1	0.05	0	0.15
	Left	0.1	0.3	0.1	0.1	0.05	1	0.2	0.3
	Right	0.1	0.15	0.2	0.3	0	0.2	1	0.25
	Up	0.1	0.05	0.05	0.1	0.15	0.3	0.25	1

Tabla A.2: Porcentajes usuarios iguales en otros movimientos o comparaciones entre los peores usuarios en función de sus EER, base de datos Serwadda, modo portrait.

		Intra-session				Inter-session			
		Down	**Left**	**Right**	**Up**	**Down**	**Left**	**Right**	**Up**
Intra-session	**Down**	1	0.25	0.13	0	0.38	0.13	0	0.13
	Left	0.25	1	0.13	0.13	0.13	0.13	0.13	0.13
	Right	0.13	0.13	1	0	0.25	0.25	0.63	0
	Up	0	0.13	0	1	0.13	0.25	0.25	0.38
Inter-session	**Down**	0.38	0.13	0.25	0.13	1	0.25	0.13	0.25
	Left	0.13	0.13	0.25	0.25	0.25	1	0.38	0
	Right	0	0.13	0.63	0.25	0.13	0.38	1	0
	Up	0.13	0.13	0	0.38	0.25	0	0	1

Tabla A.3: Porcentajes usuarios iguales en otros movimientos o comparaciones entre los mejores usuarios en función de sus EER, base de datos Serwadda, modo landscape.

		Intra-session				Inter-session			
		Down	**Left**	**Right**	**Up**	**Down**	**Left**	**Right**	**Up**
Intra-session	**Down**	1	0.13	0	0.25	0.5	0.13	0.13	0.38
	Left	0.13	1	0.38	0.13	0	0.75	0.25	0.13
	Right	0	0.38	1	0	0	0.5	0.13	0.13
	Up	0.25	0.13	0	1	0.13	0.13	0.13	0.63
Inter-session	**Down**	0.5	0	0	0.13	1	0.13	0	0.38
	Left	0.13	0.75	0.5	0.13	0.13	1	0.25	0.13
	Right	0.13	0.25	0.13	0.13	0	0.25	1	0
	Up	0.38	0.13	0.13	0.63	0.38	0.13	0	1

Tabla A.4: Porcentajes usuarios iguales en otros movimientos o comparaciones entre los peores usuarios en función de sus EER, base de datos Serwadda, modo landscape.

		Desarrollo				Test			
		Down	**Left**	**Right**	**Up**	**Down**	**Left**	**Right**	**Up**
Desarrollo	**Down**	1	0.43	0.29	0.43	0.43	0	0.14	0.29
	Left	0.43	1	0.57	0.29	0.43	0.43	0.43	0.29
	Right	0.29	0.57	1	0.29	0.43	0.43	0.43	0.43
	Up	0.43	0.29	0.29	1	0.43	0.14	0.14	0.43
Test	**Down**	0.43	0.43	0.43	0.43	1	0.14	0.29	0.43
	Left	0	0.43	0.43	0.14	0.14	1	0.43	0.14
	Right	0.14	0.43	0.43	0.14	0.29	0.43	1	0.29
	Up	0.29	0.29	0.43	0.43	0.43	0.14	0.29	1

Tabla A.5: Porcentajes usuarios iguales en otros movimientos o comparaciones entre los mejores usuarios en función de sus EER, base de datos UMDAA-02, modo portrait.

		Desarrollo				Test			
		Down	**Left**	**Right**	**Up**	**Down**	**Left**	**Right**	**Up**
Desarrollo	**Down**	1	0.14	0.14	0.14	0.29	0	0.29	0.29
	Left	0.14	1	0.14	0.14	0.14	0.29	0.43	0.14
	Right	0.14	0.14	1	0.29	0.29	0	0.43	0.29
	Up	0.14	0.14	0.29	1	0	0.14	0.43	0.29
Test	**Down**	0.29	0.14	0.29	0	1	0.29	0.29	0.43
	Left	0	0.29	0	0.14	0.29	1	0	0.14
	Right	0.29	0.43	0.43	0.43	0.29	0	1	0.43
	Up	0.29	0.14	0.29	0.29	0.43	0.14	0.43	1

Tabla A.6: Porcentajes usuarios iguales en otros movimientos o comparaciones entre los peores usuarios en función de sus EER, base de datos UMDAA-02, modo portrait.